高等学校计算机系列规划教材

离 散 数 学

（第3版）

马叔良 主编

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

离散数学和微积分不同，离散数学是以离散对象为研究对象的，是计算机专业和其他一些工程专业的数学基础。本书包含了数理逻辑、集合论、数函数和递推关系、图论、代数系统及布尔代数等主要内容。本书注重理论的系统性和准确性，特别重视对理论难点的诠释，叙述通俗易读。

本书适合作为高等学校计算机专业或其他工程类专业教材使用，也可以供对离散数学有兴趣的读者自学。

图书在版编目（CIP）数据

离散数学/马叔良主编. —3 版.—北京：电子工业出版社，2009.11
（高等学校计算机系列规划教材）
ISBN 978-7-121-09729-4

Ⅰ. 离… Ⅱ. 马… Ⅲ. 离散数学—高等学校—教材 Ⅳ.O158

中国版本图书馆 CIP 数据核字（2009）第 189119 号

责任编辑：吕 迈
印 刷：
装 订：
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1 092 1/16 印张：12.75 字数：326 千字
印 次：2009 年 11 月第 1 次印刷
印 数：0 000 册 定价：20.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

改革开放三十年来，我国经济高速发展。当今，在激烈的国际竞争环境下，从劳动密集型向技术集约型的经济结构转型成了当务之急。而人才问题是这次转型成败的一个关键因素，教育首当其冲。近年来，创新型的科学技术研究和生产链的两端——合格的从事基础理论研究和高级技术生产的人才奇缺已经成为制约我国生产力发展的一大问题。无论从理论上考虑，还是从一些成功的高级技术人才的经验来看，培养具有必要的理论基础和善于把理论知识应用到生产实践的创新型人才是我们高等教育的培养目标。除却少数培养基础理论研究人才的纯理科专业外，高等教育既不能是理论脱离实际的“纯理论”教育，也不能是为某一生产线所谓“对口岗位”培养高级操作人员的培训班。我们始终认为，掌握必要的理论知识并且善于用理论指导实践的科技人才才是当今我国经济建设所需要的。

数学作为一切科学的基础是不言而喻的事实，只是不同的学科领域更加密切地依重数学的某一些分支而已。计算机科学和某些工程学科则是以“离散数学”作为其主要的研究工具。一是因为目前使用最广泛的各种架构的机器都是所谓“数字模式”的，即这种机器的内部有且仅有两种不同的信息元，在硬件内用高、低电平或者介质的不同磁化方向或晶相等加以记录，数学上用“离散量”0 和 1 对这两种信息元加以描述（抽象的对应物）。二是因为当今通过计算机运算的绝大多数课题，要么直接就是基于若干离散对象之间的种种联系，要么就是将一个或简单或复杂的连续变量之间的关系，通过所谓的数值分析的方法用相应的离散变量近似地加以描述，并且这种近似的精度是可以以计算量的增大来换取的。譬如，简单到连续函数图形下的曲边梯形面积的求解，复杂至飞行器的空气动力外形的网格设计方法等，都是处理离散变量的过程。三是因为计算机的软、硬件系统本身就是一个有限结构或有限离散结构。

本书是为计算机科学等专业的学生写的一本离散数学基础教材。理论部分取材于数学的几个与计算机学科联系紧密的理论分支，并且在不致与其他课程内容重复的宗旨下，尽可能地给出了一些运用数学理论解决专业问题的实例。

我们认为，同一门课程，不论是本科还是专科，在介绍其基本概念、术语和基本理论方面，同样需要做到严缜性和系统性。因为这些概念、术语和基本理论构成离散数学的理论体系，是准确理解和掌握离散数学的基石。本教材正是基于这样的理解来安排教学内容的。虽然教材的各章内容取材于若干数学分支，通过仔细的考虑安排了一个合理的次序，使之前后呼应，并以数理逻辑为论证工具贯穿全书，希望借以培养学生的逻辑思维能力。尽管如此，我们还是不打算使本书包含离散数学的所有内容。本书省略了数值分析、组合学、概率等理论的内容，这主要是考虑到学生在他们不同阶段的学习中会涉猎这些知识。

学习离散数学并非必须以数学分析等其他高等数学的知识作为准备，只要有一个勤于思考、善于分析问题的好习惯就行。本教材的很多专题都是从日常生活问题引出的，并有大量的例题和练习，行文也力求通俗，包含了供读者进一步研修离散数学或其中部分专题的较全面的基础知识，可供希望了解离散数学内容的读者自学之用。本书配有电子教案和部分习题解答，可在电子工业出版社华信教育资源网（www.huaxin.edu.cn）免费下载。

本教材由马叔良老师主编，顾豫、田立炎和周良英老师先后参加了编写工作。

我要特别感谢北京大学力学系陈耀松教授和马瑜教授，他们耐心地审阅了本书并提供了许多极有价值的意见。

在此，我还要感谢我的女儿马谨，她花去了大量的业余时间完成并完善了本书的所有图稿。

此次修订基本保持了前一版的结构和内容，仅对部分文字做了修改或增删。作者固然殚精竭虑，希望本书修订版本更加完美，然而想必仍然会有不尽完善之处。作者竭诚希望读者和专家不吝赐教。

马叔良

2009 年 8 月于苏州

目　录

第1章 绪 论

1.1 离散数学的研究对象

“离散数学”是一门相对于“连续数学”而命名的数学分支。数学分析和复变函数是以函数为主要研究对象的。在那里，函数这一概念是指一个（或多个）连续变量和另一个连续变量之间的对应关系，连续变量在一个确定的范围内变化（取值）。离散数学也研究函数（和关系），可是一般而言，这里主要讨论的是“离散量”的结构及其对应关系。

所谓“离散量”（或离散对象）是一个很普遍的概念，一般来说一个离散变量可取到有限个或无限可列[*]个值。这正是与计算机本身结构和用计算机可处理（解决）的问题的有限性及对象的离散性相一致的。

下面是现实世界中一个可以用计算机处理（运算）的问题被求解的线索，为我们提供了离散数学处理这类问题的数学方法的最初印象。例如，一个旅行社拟新辟一条旅游线路：从旅行社所在城市出发，巡回其余 n-1 个城市（或景点），最后返回出发地。当然，旅行社必须考虑它的经济效益和游客一般不愿在一次旅行中两次光顾同一城市的愿望。那么，它应该如何设计它的这条旅游线路呢？诚然，如果在这条线路上存在不太多的景点时，人们并不一定要依赖计算机来解决这个问题。他们可以在纸上画出 n 个小圆圈（或点）表示上述这 n 个城市或景点，再用连接两个小圆圈的线段（直线段或曲线段都无所谓）表示该两端点间实际存在的一条交通线。现在，剩下的问题就是看你能否用一支铅笔，从代表起点的小圆圈开始，沿着图上已有的线段，将其余 n-1 个小圆圈每个画过一次且仅画过一次并最后回到起点。也许，旅行社的工作人员这样试了不多的几次就找到了一条符合要求的线路。但是，也许他们用掉了很多很多纸，甚至于磨掉了一支铅笔也没能设计出这样的线路来！因为，很可能这样的线路根本就不存在。而离散数学的理论对这个问题很可能只需一个很简单的计算就知道这条路线是不存在的了（这是一个所谓的哈密尔顿问题，将在第 5 章图论中讨论）。

回过去再看一看这个旅游线路的问题，它的解决（求得解或是证实无解）过程经过了以下几个阶段：首先是将 n 个城市和连接它们的交通线绘制成一幅由点和线组成的图。这是人们解决问题的第一步抽象，或者说是建立待解问题的“数学模型”。它将现实世界中的对象即城市和交通线抽象成了小圆圈和线段这样一些离散对象。这是解决问题的本质的一步（至少对旅行线路这一特殊问题是本质的）：从每一个城市直接可抵达的有哪些城市。完全不必关心诸如某一城市的人口、气候等其他与本问题无关的属性。有了对现实世界正确的完整的（对需要解决的问题是充分的）抽象，第二步就是将现实问题转化为一个数学问题。最后的步骤就是用数学方法（和理论）求解问题的答案或证明问题无解。

有了解决上面那个旅行线路的经验，我们再来看一个实际问题：有 N 个人要参加一个圆桌午宴。为活跃气氛，主办方希望每位来宾的左右邻座都是他（她）的朋友。初看起来这个问题和上面那个问题几乎没有什么相似之处，其实不然。如果我们仍然用一个小圆圈来代表问题中的某位来宾；而用一根线段连接两个小圆圈，表示这两个圆圈所代表的两位来宾是朋友关系。那么，你现在看到了什么？是一个有 N 个圆圈和一些连接它们中的某些圆圈的线段

[*] 集合{0,1,2,…}就是我们最熟悉的无限可列个元素的集。

的图形。而最终问题的解决竟然和上述旅行线路问题是完全一样的！

通过以上这两个简单例子，我们试图向读者说明两件事：一是数学（当然也包含离散数学）的抽象为什么常常可以用来解决不同类型的实际问题；二是某些离散对象的问题，必须被正确地抽象为一个离散数据结构及其关系的模型。解决这类问题的有力工具无疑非离散数学莫属了。

1.2 离散数学的主要内容

离散数学作为一门大学课程，在国外最早大约是 20 世纪 70 年代的事了。当时，一些主攻计算机科学的学生感到自己的数学基础不足以很好地学习和解决本专业的许多问题，于是就有一些计算机科学家根据自身对计算机科学的理解，与一些数学家一起圈定了一些他们认为对计算机科学是必需的数学专题，结合计算机科学中的一些实例编著了一些主要是命名为“离散数学结构和方法”或“离散数学基础”之类的讲义和书籍，开设相应的课程供大学里学习计算机专业和其他一些相关工程专业的学生选修。由于反映很好，渐渐在各计算机专业中，将“离散数学”作为必修课来开设。我国大约是在 20 世纪 80 年代初期，从翻译国外离散数学专著开始，逐渐由各著名工科院校的教师编写了一些适合我国教学情况的离散数学教材，并在计算机科学系中开设了相应的课程。

如上所述，由于各专家主攻计算机的方向和他们对计算机教学的理解不尽相同，因此，在“离散数学”名下的内容也不完全一样。不过，经过这些年的教学实践，对于计算机专业所需的离散数学内容渐渐有了比较统一的认识，即包括四大部分：数理逻辑、集合论和关系、图论初步及代数系统。本书也以这些内容为主要架构，同时添加了诸如离散数函数和递推关系等很有用的内容，基本上已涵盖了适合计算机专业所需的数学内容。

1.3 学习离散数学的方法

离散数学是计算机科学系所有专业的基础数学课程，一方面有其实用性（应用数学的特征），另一方面有其本身作为数学基础课的严谨的理论性。所以，学习任何一个专题时，首先要精确严格地掌握好每一个概念和术语，正确理解它们的内涵和外延。因为公理、定理或定律的基石都是概念。只有正确地理解了概念，才能把握定理的实质，才能熟练地将公理、定理应用于解决问题。完全地、精确地掌握一个概念的好办法是首先要深刻理解概念的内涵，然后举一些属于和不属于该概念外延的正、反两方面的实例。如果对一些似是而非的例子也能辨别的话，应该说这个概念是真正被理解了。对一些重要的概念，能记住一两个实例也很管用，这对牢固掌握一个概念是很有好处的。

必须提醒读者的是，千万不要在完全理解某些概念、基本定理之前就匆忙地去做相应的习题。几乎可以肯定地说，这样做是不能学懂离散数学的，更无法应用它。

总的说来，我们建议读者养成一种自觉的学习习惯，就是首先要掌握好基本概念和术语，在此基础上理解每一基本定理的本质，最后通过学习和借鉴书中提供的例题，独立地完成每一次作业。并且，每次作业完成之后，能自觉地归纳出其中用到的基本解题方法。

虽说离散数学是一门很抽象的课程，但是只要读者肯动脑筋思考，掌握正确的学习方法，那么一定会在以后的学习中体会到越学越轻松的感觉。一般而言，毕竟学习离散数学只需要有一定的中学数学基础就够了。

第2章　数 理 逻 辑

推理是人类特有的思维活动。人们在社会实践中自觉或不自觉地通过感官接受外界的消息形成所谓**表象**，同类表象的反复出现在人脑中建立起一个**概念**。概念已不再囿于个别的表象而具有一类表象的本质**属性**，这就是概念的**内涵**。反过来说，所有归纳出该概念的具有特定表象的事物（对象）组成了概念的**外延**。例如，人们在品尝了苹果、梨、香蕉等之后，将具有各种特定香味而富含营养和水分的植物果实概括为“水果”这一概念。客观世界里实际并不存在具体的一个水果，但水果这一概念却包涵了每一个苹果、梨、香蕉等。因此，我们说概念是存在于人脑里的对现实世界对象的一种抽象，它只存在于人的思维中。而水果这一概念的外延却是由客观世界中存在的所有有水果属性的个体组成的。我们可以向别人展示一只梨，并对他说：这是一只梨，它是一种水果（严格地说，他应当说这是水果中的一个）。但任何人都无法展示水果是什么。这就是说，概念存在于思维之中，而概念的外延存在于客观世界。当然，以上的叙述只是为了使大家明白概念是怎样产生而举的一个特殊例子。现实生活中还有很多“抽象的概念”，如时间、空间、数学上的点等。事实上，我们根本不可能找到一个只有位置而无大小的几何点。但是，我们照样可以完美地将所有的实数和几何上的一根有方向的直线，即所谓数轴对应起来。于是我们要对前面提到的“外延存在于客观世界”一语做一些补充说明。通常，在科学技术领域里，人们在研究某些现象时发现，必须对某些客观实体做出更为抽象的概括，摒弃客体的某些属性，张扬它的局部属性，形成一种全新的概念。这样做了，往往可将被研究事物的本质属性突现出来。例如，几何上的点就是从具有一定大小的普通的点，通过忽略其大小而强调其几何位置所得的。这样做了，就使得实数理论建立在一个有形的对应物——数轴上了。不要低估了这样做的影响。从此，几何学与代数学建立起密切的联系，使得解析几何、画法几何、微分几何得以借助分析手段长足地发展起来。所以说，“概念的外延存在于客观世界”一语的正确理解应当是：人们不可能杜撰一个根本不反映任何客观事物本质属性的概念。如果有这样的概念，那只能存在于迷信或神话中。

概念还不是人类思维的全部，**判断**是人们更具创造力的思维活动。所谓判断，就是对某些概念之间的必然联系做出的断言。判断的真实性最终只能为客观实践所证实或否定。这就是我们通常说的“实践是检验真理的唯一标准”。数理逻辑主要研究的就是如何从一组已知判断，通过所谓**有效推理**而最终获得一个全新判断的逻辑学分支。

说到有效推理，这是一组明确规定的**法则**，允许从一个或一组已知判断，得到一个新的判断。特别要强调的是：有效推理是经过反复实践认证符合客观规律的一种人类的正确思维法则。但它只保证推理本身是正确的，并不能保证推理的结果——最终得出的判断也正确。因为如果作为推理前提的判断是虚假的或局部是虚假的话，即使推理过程是有效的，我们也不能保证结论一定是正确的。我们唯一可以保证的是在正确的前提下，经过有效推理必定产生正确的结果。

逻辑学是一门研究人类思维规律的科学。由于它的普遍适用性，所以推理规则应当被表述为与任一具体的论证或学科的内容无关。这使逻辑学必须使用一种所谓**形式语言**，它是由

完全定义了的概念或术语以及如何使用这些概念的语法组成。再则，为不让形式语言有**二义性**，我们使用有明确定义的符号来表示形式语言中的那些概念，使得形式语言被描述成类似于数学公式的样子。因此，有时我们也称之为**符号逻辑**。

最后，提醒读者事先警惕这样一个明显的困惑，即在定义和描述无二义性的形式语言之前，我们有的只是日常生活中使用的语言（如汉语、英语等），这种语言常称之为**元语言**。元语言不乏二义性（大家都知道双关语）。用一种并非严格的自然语言来定义或描述一种精确而无二义性的语言，这种困难一开始就应充分留意。

2.1 命题

2.1.1 命题的概念

命题逻辑中的基本**语素**是**命题**。在形式语言中，如下定义的**陈述语句**是命题：

定义 2.1 命题就是在特别指定的范围、时间和空间内，具有唯一确定的真假性的陈述语句。

由于在命题逻辑中只讨论有确定真假性的陈述语句，并不关心语句本身的语义是什么，所以“语句”一词与“命题”被等价地使用。

定义 2.2 在特定的范围、时间和空间内，真实的命题具有“真”的**真假值**。反之，虚假的命题具有“假”的真假值。

命题的真假值通常简称为**真值**。真值“真”也可以用符号 **T**（TRUE）或 **1** 来表示；“假”可以用 **F**（FALSE）或 **0** 来表示。为书写方便，在不致引起混淆的情况下，**T**,**F**,**1**,**0** 也可以不表示成黑体，并以此作为本书的约定。

值得指出的是，一个命题的真值总是确定存在的（非真即假，反之也然，别无其他）。它与我们的主观感受和是否知道这个真值完全无关。

例如，有如下命题：

（1）宇宙中必然存在除人类以外的智慧生物。

人类还无法判断这个命题是真是假。但是其确实具有确定的真假性，这是肯定的。

另一值得一提的是，真值通常与论述一个命题的范围、时间和空间有关。例如：

（2）101+1=110。

这个命题在二进制计数制下是真的，在其他计数制下则为假。然而在论述命题的上下文中，通常总可以确定它是在二进制范围内给出的。

定义 2.3 除却其本身之外，它的任何局部都不是命题，这样的命题叫**原子命题**。

定义 2.4 由两个或两个以上命题通过联结词和圆括号组成的命题是**复合命题**。

“联结词”在下一节讨论。

2.1.2 命题的表示

原子命题与复合命题的共同特点是它们均有唯一的真值。在不必要研究一个命题的结构时，它们都被笼统地称为“命题”，都可以用大写的字母，如 $A,B,C,\cdots,P,Q,R$ 等表示。也可用字母加下标的方式表示不同的命题，如 $P_1,P_2,\cdots,P_i$ 就表示 i 个不同的命题。

（3）*P*：天下雪了。

这里，把符号“*P*”看成了命题“天下雪了”的等价物。这种表示命题的符号被称做**标识符**。

应该特别指出，标识符在上面都是被用来表示某一特定的命题。标识符还有一个用法，就是一个标识符并不具体代表一个命题，而是表示在它所在的位置上可以用某一确定的命题去代替它。这种替代，通常叫**指派**。如前所述，由于在命题逻辑里，一般并不关心命题的语义，只关心其真假值。所以明白地说，对一个标识符的指派，实际上就是给它一个 T 或 F 这样的真假值。

归纳一下，在上面提到的标识符第一种用法中，它称为一个**命题常量**；而第二种用法的标识符叫做**命题变量**（元）。命题变元在对其指派前不是命题，没有真值。

一个符号究竟是命题常量或者变量是不会引起混淆的，因为在它们出现的环境中均会得到说明。

在很多文献中，一个命题之前冠以一个用圆括号封闭起来的数字，并用它代表这个命题。如上文中（2）就可以用来代表命题“101+1=110”。

下面是另一些命题：

（4）上海是一个国际大都市。

（5）2020 年人类将踏上火星。

（6）哥伦布发现了美洲大陆。

（7）罗马是法国的首都。

（8）费城是一个古老的城市。

这些命题中，（4）、（6）的真值是 **T**，（7）的真值是 **F**，（5）的真值目前尚无法确定，（8）在美国这个只有 200 多年历史的国家里是真的，而对于一些有数千年文明史国家的人来说是假的（我们说过，命题的真值是在指定的范围、时间和空间中确定的）。

而下来的两个语句不是命题：

你就别去了吧。

DNA 为什么被称为生命的密码？

因为前一个语句是祈使句，后一个是疑问句。对它们讨论真假性是无意义的。

最后我们给出一个语句：

托马斯为本镇所有自己不刮脸的男人刮脸。

这是一个**悖论**。他不可能有真假值。因为托马斯这个（男）理发师，无论他是否为他自己刮脸，都与上述陈述句发生矛盾。关于悖论的规避，我们在第 3 章里给出了一个习题，在那里会对此做一些说明。

2.2 命题联结词

联结词是用来将（原子）命题联结成复合命题的一种基本语素。自然语言中也有联结词（或、和、……），通常由词或短语组成。可是它们经常产生二义性。如“他有钢笔或铅笔”，究竟是说某人只有钢笔或铅笔二者之一呢？抑或兼有二者呢？通常我们是不能肯定的。本节我们就来为逻辑联结词定义，并给予符号化。

有必要再次强调的是，以下的标识符作为命题变元使用。因此，在对一个符号表达式中

的每一个标识符指派之前，它不可能有真值，因此这种表达式不是一个命题，我们称之为**命题公式**。对一个命题公式中每一标识符均指派一个命题之后，原来的命题公式成为复合命题。这时，它有一个确定的真值。

通常，我们把对一个命题公式中的每一个变元均指派一个真值的做法，称做对命题公式的一次**指派**。因此我们说，仅当对命题公式做了指派之后，命题公式才是一个复合命题。

2.2.1 联结词的定义

定义 2.5 设 P 是一个命题，则 P 的**否定**也是命题，记为“$\neg P$”，读做“非 P”。

$\neg P$ 为假，当且仅当 P 为真。

“否定”的定义也可以用表 2.1 给出。

表 2.1 否定的真值表

P	$\neg P$
F	**T**
T	**F**

【例 2.1】 设 P：伦敦是一个多雾的城市。

那么，$\neg P$ 表示的命题是：

$\neg P$：并非伦敦是一个多雾的城市。

或者

$\neg P$：伦敦不是一个多雾的城市。

虽然以上两个自然语言的语句形式上有所不同，但它们的真值完全相同。读者从此也可看出符号化的语言是如何消除语言的二义性的。

“否定”只是对一个语句的修饰，习惯上仍称做联结词。有时也说它是**一元联结词**或**一元运算**。因为一个语句在用“否定”修饰后生成一个意义和真值完全不同的新语句。

定义 2.6 设 P,Q 是两命题，则 P,Q 的**合取**是一个新的命题，记为“$P \wedge Q$”，读做“P 与 Q”或者“P 且 Q”。$P \wedge Q$ 为真，当且仅当 P 为真且 Q 也真。

合取的定义也可以用表 2.2 给出。

表 2.2 合取的真值表

P	Q	$P \wedge Q$
F	**F**	**F**
F	**T**	**F**
T	**F**	**F**
T	**T**	**T**

【例 2.2】 构造以下两个语句的合取。

P：这房子很大。

Q：2+2=4。

解 $P \wedge Q$：这房子很大且 2+2=4。

以上结果看起来很可笑，但从逻辑的语法规则来评判，它一点也没有错。事实上，它因沿袭了两个原子语句的真值并且有自己完全确定的真值。这反映了这样一个事实：形式语言

被表达成与所论述的内容（语义）和学科无关。在命题逻辑中，我们主要关心的只是命题的真假性。

【例 2.3】 分析以下命题中的联结词。

G：小张与小王都是三好学生。

R：小张与小王是表弟兄。

解 对于命题 *G*，我们可以引入两个原子命题：

A：小张是三好学生。

B：小王是三好学生。

于是，*G* 就可表成 $A \wedge B$。

可是对语句 *R* 而言，其中的“与”是两个名词“小张”、“小王”的联结词，而命题逻辑中的“与”仅仅是一种语句间的联结词，因此它不能用于名词的联结。实际上，语句 *R* 在命题逻辑中是原子命题，其中不含逻辑联结词“与”。

再强调一下，原子命题在命题逻辑演算中是一个最小单位，不可再细分。

定义 2.7 设 *P*,*Q* 是两个命题，则 *P* 和 *Q* 的**析取**也是命题，记为“$P \vee Q$”，读做“*P* 或 *Q*”。 $P \vee Q$ 为假，当且仅当 *P* 和 *Q* 均为假。

析取的定义也可以用表 2.3 给出。

表 2.3 析取的真值表

P	*Q*	$P \vee Q$
F	**F**	**F**
F	**T**	**T**
T	**F**	**T**
T	**T**	**T**

【例 2.4】 分析以下语句中的联结词。

（1）小张或小王是三好学生。

（2）电影院中有 400 或 500 名观众。

（3）今天下午 3:00，我在教室或阅览室。

解 语句（1）可表达成“小张是三好学生”和“小王是三好学生”两个原子命题的析取，所以语句中的“或”是命题联结词“$\vee$”。

语句（2）中的“或”不是析取联结词。该语句真正表达的意思是说，电影院里的观众数 *n* 在 400～500 人之间：$400 \leqslant n \leqslant 500$。实际人数可能是 400,401,402,…,499,500 人中的某一个值。

如果表达成如下复合命题：

（4）电影院中有 400 人或电影院里有 500 人。

这显然与原来的意义就不一样了。因此，自然语言中的“或”除作为语句联结词之外，另一种用法是表示对象的一个大致的范围。

语句（3）的“或”虽然是一个命题联结词，但是与我们先前定义的析取并不一样。因为在下午 3:00 这一时刻，“我”不可能既在教室里又在阅览室里。如果我们将原先定义的“$\vee$”称做“**可兼或**”，那么，语句（3）中的“或”称为“**不可兼或**”用“$\bar{\vee}$”表示。表 2.4 定义了不可兼或。

表 2.4　不可兼或的真值表

P	Q	$P\overline{\vee}Q$
F	**F**	**F**
F	**T**	**T**
T	**F**	**T**
T	**T**	**F**

定义 2.8　设 P,Q 是命题，则 $P\rightarrow Q$ 称为**条件命题**，读做“如果 P，则 Q”。$P\rightarrow Q$ 为假，当且仅当 P 为真，Q 为假。

条件的定义也可以用表 2.5 给出。

表 2.5　条件的真值表

P	Q	$P\rightarrow Q$
F	**F**	**T**
F	**T**	**T**
T	**F**	**F**
T	**T**	**T**

在复合语句 $P\rightarrow Q$ 中，P 称做**前件**，Q 称做**后件**。

自然语言里，有多种措辞与 $P\rightarrow Q$ 对应：

（1）P 是 Q 的充分条件。

（2）Q 是 P 的必要条件。

（3）Q，当（如果）P。

（4）P，仅当 Q，或仅当 Q，如果 P。

在表 2.5 中，后两组指派的结果与我们的预期相吻合。但前两组的指派所得结果常常令人困惑。来看语句“如果工具齐全，我们今天完成工程”。当工具齐全，我们今天完成了工程，那么该语句是真自然没有问题，即我们兑现了保证。当工具齐全而今天我们没有完成工程，则语句为假也不会引起异议，因为我们违约了。可是，当工具不齐全的情况下（前件为假），我们在今天完成了工程（后件为真）或没有完成工程（后件为假）这两种情况，我们是守约的（上面语句为真），还是违约了（语句为假）呢？为消除二义性，我们是这样定义的：

当一个条件命题 $P\rightarrow Q$ 的前件 P 为假时，不论后件 Q 为真或为假，$P\rightarrow Q$ 总是真的。我们管这叫做**善意推定**。

【例 2.5】　若函数 $f(x)$在区间(a,b)上有导数，则 $f(x)$在(a,b)上连续。

这是一个真命题。

【例 2.6】　你将一事无成，除非你努力学习。

解

设　P：你努力学习。

　　Q：你将一事无成。

于是原语句可符号化成：

　　$\neg P\rightarrow Q$

【例 2.7】　下面是一些有微妙差异的语句。

（1）我承认它，除非太阳从西方升起。

（2）我不承认它，除非太阳从西方升起。

（3）如果太阳从西方升起，我承认它。

解　设 P：太阳从西方升起。

Q：我承认它。

于是以上三个语句符号化后成为

（1）$\neg P \rightarrow Q$

（2）$\neg P \rightarrow \neg Q$

（3）$P \rightarrow Q$

因为 P 是假的，所以 $\neg P$ 是真的。这样就清楚了，语句（1）表示了“我”对某事物的坚决肯定，语句（2）表示对某事物的坚决否定。两种情况下，观点都是明确的。可语句（3）就不同了，因为它的前件 P 是假的，所以，无论“我”是否承认某事物，该语句总是真的。如果不加分析，很可能将它等同于语句（2）。看来，一个观点模棱两可，或者蓄意诡辩的人，用一个假的前件来表明自身的看法时，我们要特别注意了。

定义 2.9　设 P,Q 是命题，则 $P \rightleftarrows Q$ 称为**双条件命题**，读做“P 当且仅当 Q”。$P \rightleftarrows Q$ 为真，当且仅当 P,Q 同时有相同的真值（同时为真，或同时为假）。

双条件的定义也可以用表 2.6 给出。

表 2.6　双条件的真值表

P	Q	$P \rightleftarrows Q$
F	**F**	**T**
F	**T**	**F**
T	**F**	**F**
T	**T**	**T**

自然语言中有多种措辞与 $P \rightleftarrows Q$ 对应。

（1）P 即 Q。

（2）P 与 Q 是等价的。

（3）P 是 Q 的充分且必要条件，或者 Q 是 P 的充分且必要条件。

【例 2.8】　符号化以下语句。

（1）我上街，当且仅当你上街去。

请分析一下本语句与以下每一个语句的差别：“我上街，当你上街”，和“我上街，仅当你上街”。

（2）函数 $y = f(x)$在 $x = a$ 处连续的充分必要条件是：$f(x)$在 $x = a$ 的邻域$(a-\delta, a+\delta)$上有定义，且 $\lim\limits_{x \to a} f(x) = f(a)$，其中$\delta > 0$。

（3）1+1=2，当且仅当雪是黑的。

解答留给读者完成。

2.2.2　命题逻辑中联结词的最小集

上面定义了六种命题逻辑演算中常使用的联结词。但除了“否定”之外，其余四种并非都是必不可少的。事实上，稍后我们学习了命题公式的等价性之后就会明白这一点。通常，只用两种联结词$\{\neg, \wedge\}$或者$\{\neg, \vee\}$就可以等价地表示那些使用所有我们定义过的联结词组

成的任何命题公式。这个最小集也称为联结词的**完全集**。

若选择联结词集是{¬ ,∨}，那么

$P\wedge Q$ 也可表达为 ¬ (¬ $P\vee$¬ Q)

$P\rightarrow Q$ 可表示为 ¬ $P\vee Q$

$P\rightleftarrows Q$ 可表为 ¬ (¬ (¬ $P\vee Q$)$\vee$¬ (¬ $Q\vee P$))

对于“异或”$P\bar{\vee}Q$，因为它可以表示为¬ $P\rightleftarrows Q$，所以读者应当可写出异或仅用联结词“¬ ”和“∨”的表达式。

一般情况下，所有联结词和括号在命题公式中的优先作用次序是这样的：

1．在存在括号的情形下，内层括号优先于外层括号。命题公式在同一层次不同括号内的那些部分（子式）运算优先次序相同。

2．在无内层括号的情况下，联结词的优先次序按¬ ,∧,∨,→,⇄ 递减。

例如，在$(W\rightarrow R)\wedge(S\vee($¬ $A\rightleftarrows Q))$里，按以上规则先后起作用的联结词是¬ ,⇄,→,∨,∧（由于处于同一层括号的关系，→和∨的次序也可相反）。

2.3 命题的合式公式

上一节讨论的是用联结词生成新的、最简单的命题公式的问题。还可以由这些命题公式，通过联结词产生更复杂的公式。这一节要给出怎样的公式是在命题逻辑演算下有效的，即**合式公式**的定义。

2.3.1 合式公式

定义 2.10 按以下规则由命题标识符、括号和联结词构成的一个符号串是合式公式（wff）：

（1）单一的命题变元 P,Q 等是 wff。

（2）若 P 是一个 wff，那么¬ P 也是 wff。

（3）P,Q 均是 wff，则$(P\wedge Q)$, $(P\vee Q)$, $(P\rightarrow Q)$, $(P\rightleftarrows Q)$也都是 wff。

（4）一个符号串是一个 wff，当且仅当它可有限次地引用以上（1），（2），（3）各步骤而生成。

由此可知：

(¬ $P\wedge Q$), ¬ $(P\rightarrow Q)$, $(((P\rightarrow Q)\wedge(Q\rightarrow R))\rightarrow(P\rightarrow R))$都是合式公式，而

¬ $(P,(Q\rightarrow S)\vee R)$, $PQ\rightarrow R$

都不是 wff。

为了便捷起见，我们约定，以后一概省略最外层的括号，并将“合式公式”简称为“公式”。

2.3.2 语句的符号化

把一个由自然语言描述的命题用符号公式表达出来以避免二义性就是语句符号化。

对一个合式公式进行指派后，它就是一个复合命题。或者说，任一复合命题都可通过对某一合式公式所做的指派得出。所以，合式公式的规则自然也是判断一个复合命题有效的标准。这在语句符号化（语句翻译）时特别有用。

【例 2.9】　符号化语句“今天下午 3:00，我在教室或在阅览室”。

解　设 P：今天下午 3:00，我在教室里。

Q：今天下午 3:00，我在阅览室里。

语句被符号化为

$$P \overline{\vee} Q$$

为避免引入过多的联结词，我们也可翻译成

$$\neg (P \rightleftarrows Q) \quad 或 \quad (\neg P \rightleftarrows Q) \quad 或 \quad (P \rightleftarrows \neg Q)$$

【例 2.10】　翻译语句“晚会上，她唱歌或跳舞”。

解　设 P：晚会上，她唱歌。

Q：晚会上，她跳舞。

上述语句翻译成

$$P \vee Q \text{ 或 } Q \vee P$$

这里用了可兼或是合理的。因为整个晚会期间，她可能既唱歌了，也跳舞了。

注意语句“晚会上，她先唱歌，而后又跳舞了”是一个原子命题，与本例是不同的。

【例 2.11】　语句“小张成绩好，待人也好”。将它符号化。

解　设 A：小张成绩好。

B：小张待人好。

语句被翻译成

$$A \wedge B \quad 或 \quad B \wedge A$$

例 2.10 和例 2.11 说明了一个问题，就是合取和析取都是满足“可交换”规律的。虽然这从语义上讲得通，但我们宁肯认为这是由形式语言的语法规定的，正如前面提到的“善意推定”是为规避歧义而由语法定义一样。

【例 2.12】　语句“如果你和他不都固执己见的话，就不会发生不愉快了”。

解　设 A：你是固执的。

B：他是固执的。

C：你和他发生不愉快的事。

则语句符号化为

$$\neg (A \wedge B) \rightarrow \neg C \quad 或者 \quad (\neg A \vee \neg B) \rightarrow \neg C$$

【例 2.13】　翻译“如果你和他都不固执己见的话，不愉快就不会发生了”。

解　沿用上例的标识符，翻译成

$$(\neg A \wedge \neg B) \rightarrow \neg C \quad 或者 \quad \neg (A \vee B) \rightarrow \neg C$$

读者要细细体味以上两例的区别。

2.4　真值表、永真式和永假式

2.4.1　真值表

有时我们也用标识符表示一个合式公式。如 A 表示一个合式公式，它含有 $P_1,P_2,\cdots,P_r$ 等 r 个**原子变元**（类似于原子命题，不含任何联结词的单独的命题变元叫做原子变元）。于是可用 $A(P_1,P_2,\cdots,P_r)$表示这个公式。对它进行一个指派之后，即对 $P_1,P_2,\cdots,P_r$ 中的每一变元均指

派一个或真或假的值（命题），那么公式 A 就具有一个确定的真值。对一个有 r 个变元的公式而言，可能的不同指派有 2^r 个。将所有这些不同指派以及相应公式的真值以表格形式给出，就是它的**真值表**。

定义 2.11　设 $A(P_1,P_2,\cdots,P_r)$是 wff。对其中每一原子变元均以一个命题（真值）取代之，使之成为一个复合命题。这样的一次替代，叫做对公式 A 的一次**真值指派**。

以下是一些命题公式的真值表。

【例 2.14】　给出$\neg P\vee Q$ 的真值表。

解　见表 2.7。

表 2.7

P	Q	$\neg P$	$\neg P\vee Q$
F	**F**	**T**	**T**
F	**T**	**T**	**T**
T	**F**	**F**	**F**
T	**T**	**F**	**T**

注意该公式与条件命题 $P\rightarrow Q$ 有相同的真值表（参见表 2.5）。

【例 2.15】　给出$\neg(P\rightleftarrows Q)$的真值表。

解　见表 2.8。

表 2.8

P	Q	$P\rightleftarrows Q$	$\neg(P\rightleftarrows Q)$
F	**F**	**T**	**F**
F	**T**	**F**	**T**
T	**F**	**F**	**T**
T	**T**	**T**	**F**

同样注意该公式与“不可兼或”$P\bar{\vee}Q$ 的真值完全一样（参见表 2.4）。我们还指出，另外两个公式$(\neg P\rightleftarrows Q)$ 和 $(P\rightleftarrows\neg Q)$也有与$\neg(P\rightleftarrows Q)$一样的真值表。

【例 2.16】　给出 $P\vee(\neg P\vee Q)$的真值表。

解　见表 2.9。

表 2.9

P	Q	$\neg P\vee Q$	$P\vee(\neg P\vee Q)$
F	**F**	**T**	**T**
F	**T**	**T**	**T**
T	**F**	**F**	**T**
T	**T**	**T**	**T**

我们看到对公式的任何真值指派，公式的真值全部为“真”。

【例 2.17】　给出公式$(P\vee Q)\wedge(\neg P\wedge\neg Q)$的真值表。

解　见表 2.10。

表 2.10

P Q	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$P \vee Q$	$(P \vee Q) \wedge (\neg P \wedge \neg Q)$
F F	**T**	**T**	**T**	**F**	**F**
F T	**T**	**F**	**F**	**T**	**F**
T F	**F**	**T**	**F**	**T**	**F**
T T	**F**	**F**	**F**	**T**	**F**

该公式对所有真值指派都取“假”为真值。

2.4.2 永真式和永假式

命题公式可以分为**永假式**和**可满足**两类。**而后者又包含一类特殊的命题公式，它就是永真式**。

定义 2.12 设 A 是 wff。A 是永假式，当且仅当对 A 的任何真值指派，公式的真值均为 F。永假式也称**矛盾**。

永假式用黑体记号“**F**”表示。为书写方便可写做“F”。

以上表 2.10 对应的公式$(P \vee Q) \wedge (\neg P \wedge \neg Q)$就是一个永假式。

定义 2.13 设 A 是命题公式。A 是可满足的，当且仅当它不是永假式。

定义 2.14 设 A 是 wff。A 是永真式，当且仅当对 A 的任何真值指派，其真值均为 T。永真式也称**重言式**或**逻辑真理**。

永真式用黑体记号“**T**”表示。为书写方便，常不用黑体，就记为“T”。

从以上真值表 2.9 可知，公式 $P \vee (\neg P \vee Q)$是永真式。

有时，我们需要用一个或多个公式，去置换某一公式中的一个或多个原子变元。例如，公式

A：$P \rightarrow \neg Q$

当用公式$(W \vee Q)$置换 P 后得到一个新的公式

B：$(W \vee Q) \rightarrow \neg Q$

我们称 B 是 A 的**置换例式**。若以公式$(P \wedge Q)$置换 A 中的 Q，则得另一置换例式

C：$P \rightarrow \neg(P \wedge Q)$

再若，以$(W \vee Q)$置换 A 里的 P，同时以$(P \wedge Q)$置换 Q，则产生公式

D：$(W \vee Q) \rightarrow \neg(P \wedge Q)$

公式 D 也是 A 的置换例式，但公式

E：$(W \vee (P \wedge Q)) \rightarrow \neg(P \wedge Q)$

不是 A 的置换例式。因为这是先用$(W \vee Q)$置换 A 中的 P，得到 B 之后，再以$(P \wedge Q)$置换 B 中的 Q 产生的。

另外，$P \rightarrow (\neg J \vee R)$也不是 A 的置换例式。因为它用$(\neg J \vee R)$置换了$\neg Q$，但$\neg Q$ 不是原子变元。

定义 2.15 公式 B 是 A 的一个置换例式，当且仅当

1．若 A 中某一原子变元 P_i 被公式 S 置换，则 A 中出现的所有同一变元 P_i 也被 S 置换。

2．若 A 中若干原子变元 $P_1,P_2,\cdots,P_i$ 分别对应地被公式 $S_1,S_2,\cdots,S_i$ 置换，则这种置换必须是同时进行的。

以上第 2 条，实际上意味着各原子变元间相互是独立的，即任一变元的置换不依赖别的变元的置换。这一点很重要。

一般的置换例式没有什么意义。但永真式的任何置换例式仍是永真的；永假式的置换例式是永假的。

以永真式 $P\vee\neg P$ 为例，它的以下各置换例式都是永真式：

$(P\rightarrow Q)\vee\neg(P\rightarrow Q)$

$((P\wedge Q)\rightarrow R)\vee\neg((P\wedge Q)\rightarrow R)$

2.5 公式的等价和蕴含

设合式公式的全体由集合 F 表示。那么，在这实际上是无限个公式当中，某些公式之间是否存在着联系呢？答案是肯定的，其中最重要的是等价关系和蕴含关系。

2.5.1 公式的等价

定义 2.16 A,B 两个公式有以下情况之一，则称 A 与 B 是**等价**的，记为 $A\Leftrightarrow B$ ：

1．A 和 B 都是永真的；

2．A 和 B 都是永假的；

3．除以上两种情形之外，设公式 A 和 B 中所有共同的变元是 $P_1,P_2,\cdots,P_r$，若公式 A,B 中这 r 个相同的变元在任意相同的指派下（即对这两个公式里的每一对相同变元都用任意一个命题同时替换，而公式各自独立具有的变元用任意确定的命题替换），它们总是有相同的真值。

下面就是等价的例子。

1．$\neg\neg P\Leftrightarrow P$

2．$((P\wedge\neg P)\vee Q)\Leftrightarrow Q$

3．$(P\wedge\neg P)\Leftrightarrow(Q\wedge\neg Q)$

上述第 2 个等价关系中，两公式所含变元并不完全相同。但只要它们共同包含的变元 Q 有相同真值时，它们的真值必相等（等于 Q 的真值）。第 3 个等价关系则表示了两个无共同变元的公式，但用等价的定义来判断，它们的真值永远相同（是 F），所以也是等价的。

有多种证明公式等价的方法。用真值表直接通过定义来证明，是最基本的方法。

【例 2.18】 试证明以上第 2 个等价关系。

证明 见表 2.11

表 2.11

P	Q	$P\wedge\neg P$	$(P\wedge\neg P)\vee Q$	Q
F	F	F	F	F
F	T	F	T	T
T	F	F	F	F
T	T	F	T	T

我们将两公式的真值表按同一指派所得结果列出在同一行上的方法，清楚地看出它们是等价的。证完。

【例 2.19】 试证 $P\rightarrow Q$ 与 $\neg P\vee Q$ 是等价的。

证明　列出该两公式的真值表，如表 2.12 所示。

表 2.12

P	Q	$\neg P$	Q	$\neg P \vee Q$	$P \rightarrow Q$
F	F	T	F	T	T
F	T	T	T	T	T
T	F	F	F	F	F
T	T	F	T	T	T

上表中最后两列完全相同。证完。

【例 2.20】　试证明$(P \rightarrow Q) \wedge (Q \rightarrow P) \Leftrightarrow P \rightleftarrows Q$。

证明　列出真值表，如表 2.13 所示。

表 2.13

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	$(P \rightarrow Q) \wedge (Q \rightarrow P)$	$P \rightleftarrows Q$
F	F	T	T	T	T
F	T	T	F	F	F
T	F	F	T	F	F
T	T	T	T	T	T

以上两公式的真值表完全相同，根据定义，它们是等价的。证完。

由以上等价的基本定义，可得出另一个与它本质上一致的定义。

定理 2.1　公式 $A \Leftrightarrow B$，当且仅当 $A \rightleftarrows B$ 是永真式。

用“等价”的基本定义和双条件的定义不难证明它。证明留给读者。注意“$A \Leftrightarrow B$”是一个命题，即语句“A 与 B 是等价的”。而“$A \rightleftarrows B$”仅仅是一个公式。当且仅当命题“$A \rightleftarrows B$ 是永真式”成立时，$A \Leftrightarrow B$ 成立。换个角度说，当我们表述“$A \Leftrightarrow B$”时，是断言有两个公式 A 和 B，它们有等价的关系；但是“$A \rightleftarrows B$”只是一个用联结词连接成的复合命题公式而已。它不是一个断言或命题。

综上所述，语句“$A \Leftrightarrow B$”和语句“$A \rightleftarrows B$ 是永真式”是一回事，而“$A \Leftrightarrow B$”与“$A \rightleftarrows B$”不是一回事。

我们将经常要用到的一些基本等价关系列出在表 2.14 中，大家要熟记。

表 2.14　常用的基本等价关系

$P \wedge P \Leftrightarrow P$	$P \vee P \Leftrightarrow P$	（1）幂等律
$\neg \neg P \Leftrightarrow P$		（2）对合律
$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	（3）结合律
$P \wedge Q \Leftrightarrow Q \wedge P$	$P \vee Q \Leftrightarrow Q \vee P$	（4）交换律
$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	（5）分配律
$P \wedge (P \vee Q) \Leftrightarrow P$	$P \vee (P \wedge Q) \Leftrightarrow P$	（6）吸收律
$\neg (P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	$\neg (P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	（7）摩根律
$P \wedge T \Leftrightarrow P$	$P \vee F \Leftrightarrow P$	（8）同一律
$P \wedge F \Leftrightarrow F$	$P \vee T \Leftrightarrow T$	（9）零一律
$P \wedge \neg P \Leftrightarrow F$	$P \vee \neg P \Leftrightarrow T$	（10）否定律
$P \rightarrow Q \Leftrightarrow \neg P \vee Q$		（11）

从等价的定义直接可推知等价关系的三个初等性质：

1．若 A 是合式公式，则 $A \Leftrightarrow A$（自反性）。

2．若 A,B 是合式公式，$A \Leftrightarrow B$，则 $B \Leftrightarrow A$（对称性）。

3．若 A,B,C 是合式公式，$A \Leftrightarrow B, B \Leftrightarrow C$，则 $A \Leftrightarrow C$（传递性）。

在化简公式或证明公式等价时，经常要用另一公式对一个公式的某一子公式进行替换。因此，我们先给出子公式的定义：

定义 2.17 设 A 是合式公式。X 是取自 A 中的一个连续的子符号串，若 X 是合式的，则称 X 是公式 A 的子公式。

于是有关于替换子公式的一个定理：

定理 2.2 设 A 是 wff，而 X 是 A 的一个子公式。此外，C 是一个 wff，且 $C \Leftrightarrow X$，则以 C 代换 A 中的 X 得到的新公式 B 是与 A 等价的。

该定理的证明可参考书末列出的参考文献 2 中相应章节。

当公式包含较多的原子变元时，用真值表证公式之间等价是一件很繁冗的事。因为对有 n 个变元的公式来说，它的真值表有 2^n 行。这时，我们可以结合 2.4.2 小节中讨论过的置换例式，用定理 2.2 和等价关系的初等性质 3 来证明等价关系。

下面就是这方面的几个例子。

【例 2.21】 试证 $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R \Leftrightarrow Q \rightarrow (P \rightarrow R)$。

证明

1．先证 $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$。

首先，由定理 2.1 可知，表 2.14 所列的每一个等价式，对应有一个相应的永真式。如 $P \rightarrow Q \Leftrightarrow \neg P \vee Q$，则有对应永真式 $(P \rightarrow Q) \rightleftarrows (\neg P \vee Q)$。所以表 2.14 实际上给出了同样数目的永真式。再回忆 2.4.2 小节中讨论过的对永真（假）式的任何置换例式仍是永真（假）式的事实。所以我们现在可以说：在两个等价的公式中，以相同的公式置换它们相同变元所得的两置换例式仍然是等价的。于是，

$P \rightarrow (Q \rightarrow R) \Leftrightarrow P \rightarrow (\neg Q \vee R)$

（以 Q 置换表 2.14 的式（11）中的 P，同时以 R 置换 Q 得 $Q \rightarrow R \Leftrightarrow \neg Q \vee R$。根据定理 2.2，并以 $\neg Q \vee R$ 代换 $P \rightarrow (Q \rightarrow R)$中的等价子式 $Q \rightarrow R$）

$P \rightarrow (\neg Q \vee R) \Leftrightarrow \neg P \vee (\neg Q \vee R)$

（以 $\neg Q \vee R$ 置换表 2.14 的式（11）中的 Q）

$\neg P \vee (\neg Q \vee R) \Leftrightarrow (\neg P \vee \neg Q) \vee R$

（在表 2.14 的式（3）中，以 $\neg P$ 置换 P，$\neg Q$ 置换 Q）

$(\neg P \vee \neg Q) \vee R \Leftrightarrow \neg (P \wedge Q) \vee R$

（在 $(\neg P \vee \neg Q) \vee R$ 中，以等价子式 $\neg (P \wedge Q)$ 代换 $\neg P \vee \neg Q$）

$\neg (P \wedge Q) \vee R \Leftrightarrow (P \wedge Q) \rightarrow R$

（对表 2.14 的式（11）做置换例式：$(P \wedge Q)$置换 P。同时以 R 置换 Q）

对以上五个等价式，先后应用 4 次等价的传递性就可得到题中前两式等价的结论。

2．再证 $(P \wedge Q) \rightarrow R \Leftrightarrow Q \rightarrow (P \rightarrow R)$

$(P \wedge Q) \rightarrow R \Leftrightarrow \neg (P \wedge Q) \vee R$

$\Leftrightarrow (\neg P \vee \neg Q) \vee R$

$\Leftrightarrow(\neg Q\vee\neg P)\vee R$

$\Leftrightarrow\neg Q\vee(\neg P\vee R)$

$\Leftrightarrow Q\rightarrow(\neg P\vee R)$

$\Leftrightarrow Q\rightarrow(P\rightarrow R)$

【例 2.22】 试证$(\neg P\wedge(\neg Q\wedge R))\vee(Q\wedge R)\vee(P\wedge R)\Leftrightarrow R$

证明

左式$\Leftrightarrow(\neg P\wedge(\neg Q\wedge R))\vee((Q\wedge R)\vee(P\wedge R))$

$\Leftrightarrow(\neg P\wedge(\neg Q\wedge R))\vee((Q\vee P)\wedge R)$

$\Leftrightarrow((\neg P\wedge\neg Q)\wedge R)\vee((Q\vee P)\wedge R)$

$\Leftrightarrow(\neg(P\vee Q)\wedge R)\vee((Q\vee P)\wedge R)$

$\Leftrightarrow(\neg(P\vee Q)\wedge R)\vee((P\vee Q)\wedge R)$

$\Leftrightarrow(\neg(P\vee Q)\vee(P\vee Q))\wedge R$

$\Leftrightarrow \mathrm{T}\wedge R$

$\Leftrightarrow R$

【例 2.23】 试证$((P\vee Q)\wedge\neg(\neg P\wedge(\neg Q\vee\neg R)))\vee(\neg P\wedge\neg Q)\vee(\neg P\wedge\neg R)$是永真式。

证明

原式$\Leftrightarrow((P\vee Q)\wedge(P\vee\neg(\neg Q\vee\neg R)))\vee\neg(P\vee Q)\vee\neg(P\vee R)$

$\Leftrightarrow((P\vee Q)\wedge(P\vee(Q\wedge R)))\vee\neg((P\vee Q)\wedge(P\vee R))$

$\Leftrightarrow((P\vee Q)\wedge((P\vee Q)\wedge(P\vee R)))\vee\neg((P\vee Q)\wedge(P\vee R))$

$\Leftrightarrow((P\vee Q)\wedge(P\vee R))\vee\neg((P\vee Q)\wedge(P\vee R))$

$\Leftrightarrow \mathrm{T}$

最后一步，是用$(P\vee Q)\wedge(P\vee R)$置换$P\vee\neg P\Leftrightarrow \mathrm{T}$里的变元$P$得出的。

2.5.2 公式的蕴含

蕴含是一种较等价更为普遍的关系。

定义 2.18 设公式A和B中所有共同的变元是$P_1,P_2,\cdots,P_r$。若公式A,B在上述r个相同变元在任意相同指派下（其含义同定义 2.16），当A为真时，B也必定为真，则称A蕴含B。记为“$A\Rightarrow B$”。

由以上定义不难看出，每一个永真式均蕴含永真式。

以下是一些蕴含的例子。

（1）$P\Rightarrow P\vee Q$

（2）$R\Rightarrow(\neg P\vee P)$

（3）$(\neg P\wedge P)\Rightarrow R$

（4）$P\rightarrow Q\Rightarrow\neg P\vee Q$

其中，式（2）中的$\neg P\vee P$是永真的，由蕴含定义还可知：任何公式蕴含永真式。式（3）中的$\neg P\wedge P$是一永假式，所以任何公式被永假式所蕴含。而式（4）中的两公式是等价的，但确实它们中的任何一个都蕴含另一个，即一个等价式实际上隐含两个蕴含式。

定理 2.3 公式A蕴含B，当且仅当$A\rightarrow B$是一个永真式。

像等价的第二个定义那样，我们要分清$A\Rightarrow B$是一命题，而$A\rightarrow B$只是一个公式。

证明一个蕴含关系 $A \Rightarrow B$，可先假设 A 为真，然后推出 B 必为真。例如，要证 $P \wedge (P \rightarrow Q) \Rightarrow Q$，可设 $P \wedge (P \rightarrow Q)$为真，于是有 P 为真和 $P \rightarrow Q$ 为真，最后可知 Q 必为真。

表 2.15 是一些基本的蕴含关系。

表 2.15　常用的基本蕴含关系

$P \wedge Q \Rightarrow P$，$P \wedge Q \Rightarrow Q$	（1'）
$T \rightarrow P \Rightarrow P$，$P \rightarrow F \Rightarrow \neg P$	（2'）
$P \Rightarrow P \vee Q$	（3'）
$\neg P \Rightarrow P \rightarrow Q$	（4'）
$Q \Rightarrow P \rightarrow Q$	（5'）
$\neg (P \rightarrow Q) \Rightarrow P$，$\neg (P \rightarrow Q) \Rightarrow \neg Q$	（6'）
$P \wedge (P \rightarrow Q) \Rightarrow Q$	（7'）
$\neg Q \wedge (P \rightarrow Q) \Rightarrow \neg P$	（8'）
$\neg P \wedge (P \vee Q) \Rightarrow Q$	（9'）
$(P \rightarrow Q) \wedge (Q \rightarrow R) \Rightarrow P \rightarrow R$	（10'）
$(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R) \Rightarrow R$	（11'）
$(P \rightarrow R) \wedge (Q \rightarrow S) \Rightarrow (P \wedge Q) \rightarrow (R \wedge S)$	（12'）
$(P \rightarrow R) \wedge (Q \rightarrow R) \Rightarrow (P \vee Q) \rightarrow R$	（13'）
$(P \rightarrow Q) \wedge (P \rightarrow R) \Rightarrow P \rightarrow (Q \wedge R)$	（14'）

以上蕴含关系均可通过定理 2.3 证明之。

定义 2.19　设有条件命题 $A \rightarrow B$。

1．相对于 $A \rightarrow B$，命题 $B \rightarrow A$ 称之为**逆换式**。

2．相对于 $A \rightarrow B$，命题$\neg A \rightarrow \neg B$ 称之为**反换式**。

3．相对于 $A \rightarrow B$，命题$\neg B \rightarrow \neg A$ 称之为**逆反式**。

定理 2.4　公式$\neg B \rightarrow \neg A$ 为真，当且仅当 $A \rightarrow B$ 为真。

证明

必要性。设$\neg B \rightarrow \neg A$ 为真，则可分成两种情况讨论：

（1）$\neg B$ 为真，则$\neg A$ 为真，于是 A 为假，于是 $A \rightarrow B$ 为真。

（2）$\neg B \rightarrow \neg A$ 为真，$\neg B$ 为假，于是 B 为真，于是 $A \rightarrow B$ 为真。

类似地，可证明充分性。

由此可知，$A \Rightarrow B$ 与$\neg B \Rightarrow \neg A$ 是一回事。有时要证 $A \Rightarrow B$ 必须分多种情况讨论，如果我们可较简单地证明$\neg B \Rightarrow \neg A$，那么 $A \Rightarrow B$ 自不成问题。

【例 2.24】　试证 $P \Rightarrow Q \vee \neg (P \rightarrow Q)$

证明 1

设 P 为真，来证 $Q \vee \neg (P \rightarrow Q)$为真。

（1）若同时 Q 为真，则 $Q \vee \neg (P \rightarrow Q)$为真。

（2）若 Q 为假，则 $P \rightarrow Q$ 为假，得$\neg (P \rightarrow Q)$为真，于是 $Q \vee \neg (P \rightarrow Q)$为真。

证明 2

设 $Q \vee \neg (P \rightarrow Q)$为假，来证 P 为假。

事实上，此时必有 Q 为假和 $P \rightarrow Q$ 为真，于是 P 为假。

蕴含关系也有三个基本性质：

1．若 A 是 wff，则 $A \Rightarrow A$（自反性）。

2．若 A,B 都是 wff，且 $A \Rightarrow B$ 和 $B \Rightarrow A$，则 $A \Leftrightarrow B$（反对称性）。

3．若 A,B,C 都是 wff，且 $A \Rightarrow B$ 和 $B \Rightarrow C$，则 $A \Rightarrow C$（传递性）。

特别指出，以上性质 2 的逆命题也成立，于是有：

定理 2.5　设 A,B 都是合式公式。A 和 B 等价，当且仅当 A 蕴含 B 并且 B 蕴含 A。

因此，理论上说，表 2.14 所列的等价式除交换律以外，都相当于两个对应的蕴含关系（因为 $P \wedge Q \Rightarrow Q \wedge P$ 与 $Q \wedge P \Rightarrow P \wedge Q$ 互为置换例式）。

重要的是：在具有蕴含关系的两个公式中，用相同的公式去置换它们中相同的变元，所得的两个置换例式仍保持原有的蕴含关系。例如，$P \Rightarrow P \vee Q$，所以 $(R \vee S) \Rightarrow (R \vee S) \vee Q$。

2.6　公式的主范式

由 2.3 节合式公式的生成法则可知，n 个变元可组成实际上无限个形式不同的公式，它们组成一个无限集合 F。

问题是这个无限集 F 有怎样的结构呢？通过本节的讨论可以完全地回答这个问题。下面的讨论揭示了合式公式的本质属性：所有彼此等价的公式都与唯一的一个形式规范、结构统一的所谓主范式等价。而对于 n 个变元的公式来说，这样的主范式 $C_i(i=1,2,\cdots,2^{2^n})$ 有且仅有 2^{2^n} 个。

换一个角度来说就是：可以将含 n 个变元的公式的无限集 F 划分成 2^{2^n} 个子集 $F_i\ (i=1,2,\cdots,2^{2^n})$，任一含 n 个变元的公式 $C \in F$，属于某一个子集 F_i 且仅属于该子集。

2.6.1　主析取范式

本小节就来证明任一合式公式与唯一的一个主析取范式等价。让我们先给出一些概念（术语）。

定义 2.20　设 $A(P_1,P_2,\cdots,P_n)$ 是一合式公式。$P_1,P_2,\cdots,P_n$ 是 n 个原子命题变元。所谓**初等积**就是由这些变元以及一些变元的否定组成的合取式。

例如，令 P,Q,R 是原子变元。于是 P, $\neg P$, $P \wedge Q$, $\neg P \wedge Q \wedge Q \wedge \neg R$ 都是初等积。

定义 2.21　设有公式 $A(P_1,P_2,\cdots,P_n)$。一个初等积 m 称为**小项**，当且仅当 $P_1,P_2,\cdots,P_n$ 这 n 个变元中每一个与它的否定不同时出现在其中，但两者恰出现一次。

例如，当 $n=2$，$\neg P \wedge \neg Q$, $\neg P \wedge Q$, $P \wedge \neg Q$, $P \wedge Q$ 都是公式 $P \rightarrow Q$ 的小项。而 $\neg P \wedge P \wedge Q$, $\neg P$, P, $P \wedge P \wedge \neg Q$ 这些初等积都不是小项。

显然，在一个含 n 个变元的公式中，恰好有 2^n 个不同的小项。

为讨论方便起见，事先为 n 个变元约定一个次序：$P_1,P_2,\cdots,P_n$。使每一变元（或其否定）按此次序出现在一个小项中。于是任一小项 m_i 均对应一个 n 位二进制数或**小项的编码**：编码第 j 位是 0，对应小项 m_i 中第 j 个合取项上是 $\neg P_j$，第 j 位编码是 1，对应小项 m_i 的第 j 个合取项上是 P_j。

例如，设有两变元 P,Q。它全部四个小项按编码递增次序写出来是：

$m_0=m_{00}$：$\neg P\wedge\neg Q$，$m_1=m_{01}$：$\neg P\wedge Q$

$m_2=m_{10}$：$P\wedge\neg Q$，$m_3=m_{11}$：$P\wedge Q$

若是将小项编码中的二进制编码 0 和 1 分别看成真值“**F**”和“**T**”的话，那么用一个小项的编码来指派该小项本身会如何呢？

定理 2.6 设有公式 $A(P_1,P_2,\cdots,P_n)$。其任一小项 m_i 的值为真，当且仅当以 m_i 自身的二进制编码对其施行指派。

证明是很简单的。

必要性。设 m_i 为真，由合取定义可知，m_i 的每一个合取项必为真。若第 j（j=1,2,…, n）个合取项为 P_j，则必须对它指派 **T**，于是相应指派第 j 个值为 1。若第 j 个合取项为$\neg P_j$，则必须对它指派 **F**，即相应指派的第 j 个值是 0。而这与该小项的编码第 j 位是一致的。

充分性。设以 m_i 编码去指派该小项，若第 j（j=1,2,…,n）位为 1（**T**），按编码约定，m_i 的第 j 个合取项是 P_j，于是它是 **T**。反之，若编码的第 j 位为 0（**F**），则 m_i 的第 j 个合取项是$\neg P_j$，$\neg P_j$ 也为 **T**，因为小项的全部 n 个合取项均为真，所以 m_i 为真。

在变元 P,Q 的 $2^2=4$ 个小项中，任取一个$\neg P\wedge Q$ 为例。它的编码是（0,1）。显然，以（0,1）指派$\neg P\wedge Q$ 时，得 **T**；而分别以另外三个（0,0），（1,0），（1,1）为指派，$\neg P\wedge Q$ 均为 **F**。

定义 2.22 公式 C 称为公式 A 的**主析取范式**，当且仅当

1．$C\Leftrightarrow A$；

2．C 仅是不同小项的析取式。

下面的定理实际上提供了一种用真值表来求一个公式的主析取范式的方法。

定理 2.7 一个可满足的公式 A 的主析取范式是若干小项的析取式，这些小项的编码恰与全体使得公式 A 为真的指派一一对应并相等。

证明

设 $m'_1,m'_2,\cdots,m'_k$ 是使 A 为真的指派对应的各个不同的全部小项。记 $C=m'_1\vee m'_2\vee\cdots\vee m'_k$。要证 C 是 A 的主析取范式。

显然这只要证明 $C\Leftrightarrow A$ 就好了。事实上，由这里的假设，用上述 k 个小项中任一个的编码对应的一组真值指派 C 时，C 中恰有一个小项为真（该小项具有与指派所用一组真值对应的编码，而其他 $k-1$ 个小项此时皆为假），所以 C 为真。若以某一组真值指派公式 A，A 为假，按定理假设，与此指派对应的小项必不出现在公式 C 中，于是 $m'_1,m'_2,\cdots,m'_k$ 均为假，所以 C 为假。实际上，我们已证明了以下定理：

定理 2.7 一个可满足公式的主析取范式在不记各小项次序的前提下是唯一的。

【例 2.25】 写出 $P\rightarrow Q$ 的主析取范式。

解 该公式的真值表最早在 2.2 节中给出（表 2.5）。它在指派（0,0），（0,1），（1,1）时为 **T**。所以其主析取范式为

$m_{00}\vee m_{01}\vee m_{11}$

即

$(\neg P\wedge\neg Q)\vee(\neg P\wedge Q)\vee(P\wedge Q)$

【例 2.26】 给出$\neg(P\rightleftarrows Q)$的主析取范式。

解 参阅本章 2.2 节中表 2.8，有

$\neg(P \rightleftarrows Q) \Leftrightarrow (\neg P \wedge Q) \vee (P \wedge \neg Q)$

这就是$\neg(P \rightleftarrows Q)$的主析取范式。

求主范式并不总是像上面两个例子那样简单。事实上，当一个公式包含众多的原子变元时，给出它的真值表真是一件既烦琐又容易出错的事。寻求一种相对简单而不容易出错的方法，看来是十分必要的。

下面就让我们进入如何用不断寻求一个公式的等价公式而最终求得主析取范式的讨论。当然，每一次等价变换，都要使变换后的公式在形式上更加接近主范式。先从几个例子入手。

【例 2.27】 求 $P \wedge (P \rightarrow Q)$的主析取范式。

解

$$
\begin{aligned}
P \wedge (P \rightarrow Q) &\Leftrightarrow P \wedge (\neg P \vee Q) \\
&\Leftrightarrow (P \wedge \neg P) \vee (P \wedge Q) \\
&\Leftrightarrow \mathrm{F} \vee (P \wedge Q) \\
&\Leftrightarrow (P \wedge Q)
\end{aligned}
$$

这是由唯一一个小项组成的主析取范式（要将它看成是一个小项，而不能视做一般的合取式）。

【例 2.28】 求$\neg(P \vee Q) \wedge (P \vee Q)$的主析取范式。

解

这是一个永假式。所以不可能有定义 2.22 意义下的主析取范式。

我们约定：一个永假式的主析取范式表示为 F。

【例 2.29】求$(P \vee Q) \rightarrow R$ 的主析取范式。

解

$$
\begin{aligned}
\text{原式} &\Leftrightarrow \neg(P \vee Q) \vee R \\
&\Leftrightarrow (\neg P \wedge \neg Q) \vee R \\
&\Leftrightarrow ((\neg P \wedge \neg Q) \wedge (\neg R \vee R)) \vee (R \wedge (\neg P \vee P)) \\
&\Leftrightarrow ((\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R)) \vee ((\neg P \wedge R) \vee (P \wedge R)) \\
&\Leftrightarrow (\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee ((\neg P \wedge R) \wedge (\neg Q \vee Q)) \\
&\quad \vee ((P \wedge R) \wedge (\neg Q \vee Q)) \\
&\Leftrightarrow (\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \underline{Q} \wedge R) \vee (\neg P \wedge \neg Q \wedge R) \vee \\
&\quad (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge R) \\
&\Leftrightarrow (\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge \neg \underline{Q} \wedge R) \\
&\quad \vee (P \wedge Q \wedge R)
\end{aligned}
$$

最后一步上用到幂等律，将两个相同的小项合并成一个$\neg P \wedge \neg Q \wedge R$。

下面是用等价变换的方法求主析取范式的规则。

1．用等价式 $P \rightleftarrows Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$和表 2.14 中式（11）化去公式中所有条件和双条件联结词。

2．反复利用表 2.14 中式（7）（摩根律）将否定联结词直接作用到原子变元上。

3．反复利用表 2.14 中的合取对析取的分配律，直至公式成为若干初等积的析取式。

4．所得析取式如是主析取范式则结束，否则，考查所有初等积，删去同时含有某一变元及其否定的初等积（因为该初等积为假），将初等积中那些多次出现的同一变元或同一变元的否定均分别合并成一个变元或一个变元之否定，并且合并完全相同的初等积。

5．若此时已得主析取范式则结束，否则，对不是小项的初等积，若变元 P_d 和¬ P_d 均不存在于初等积中，将此初等积与(¬ $P_d \vee P_d$)进行合 取，再利用合取对析取的分配律化成两个初等积。若需要，合并相同的初等积。返回第 5 步继续。

2.6.2 主合取范式

本小节就来证明任一合式公式与唯一一个主合取范式等价。让我们先给出一些概念（术语）。

定义 2.23 设 $A(P_1,P_2,\cdots,P_n)$是一合式公式。$P_1,P_2,\cdots,P_n$ 是 n 个变元。所谓**初等和**是由一些变元以及一些变元的否定组成的析取式。

例如，令 P,Q,R 是原子变元。P, ¬P, ¬ $P\vee Q$, ¬ $P\vee P\vee Q\vee Q$ 都是**初等和**。

定义 2.24 设有公式 $A(P_1,P_2,\cdots,P_n)$。一个初等和 M 称为**大项**，当且仅当 $P_1,P_2,\cdots,P_n$ 这 n 个变元中每一个与它的否定不同时出现，但两者恰出现一次。

例如，当 n=2,¬ $P\vee$¬ Q, ¬ $P\vee Q$, $P\vee$¬ Q, $P\vee Q$ 都是公式 $P\rightarrow Q$ 的大项。而¬ $P\vee P\vee Q$,¬ P,P,$P\vee P\vee$¬ Q 都不是大项。

显然，在一个含 n 个变元的公式中，恰好有 2^n 个不同的大项。

为讨论方便起见，事先为 n 个变元约定一个次序：$P_1,P_2,\cdots,P_n$。使每一变元（或其否定）按此次序出现在一个大项中。于是任一大项 M_i 均对应一个 n 位二进制数或大项的编码：编码第 j 位是 1，对应大项 M_i 中第 j 个析取项上是¬ P_j；第 j 位编码是 0，对应大项 M_i 的第 j 个析取项上是 P_j 。

例如，设有两变元 P,Q。它全部四个大项编码是：

$$M_0 = M_{00}:P\vee Q,\quad M_1 = M_{01}:P\vee\neg Q$$

$$M_2 = M_{10}:\neg P\vee Q,\quad M_3 = M_{11}:\neg P\vee\neg Q$$

若是将大项编码中的二进制编码 0 和 1 分别看成真值“**F**”和“**T**”的话，那么用一个大项的编码指派该大项本身会如何呢？

定理 2.8 设有公式 $A(P_1,P_2,\cdots,P_n)$。其任一大项 M_i 的值为假，当且仅当以 M_i 的二进制编码对其施行指派。

证明是很简单的。

必要性。设 M_i 为假，由析取定义可知，M_i 的每一个析取项必为假。若第 j（j=1,2,⋯,n）个析取项为 P_j，则必须对它指派 **F**，若第 j 个析取项为¬ P_j，则必须对它指派 **T**。所以，此时的真值指派必与该大项的编码一致。

充分性。设以 M_i 的编码去指派该大项，若第 j（j=1,2,⋯,n）位为 0（**F**），按编码约定，M_i 的第 j 个析取项是 P_j，于是它是 **F**。反之，若编码的第 j 位为 1（**T**），则 M_i 的第 j 个析取项是¬ P_j，¬ P_j 为 **F**，因为大项的全部 n 个析取项均为假，所以 M_i 为假。

在变元 P，Q 的 2^2=4 个大项中，任取一个¬$P\vee Q$ 为例。它的编码是(1,0)。显然，以(1,0)指派¬ $P\vee Q$ 时，得 **F**；而以另外三个（0,0），(0,1)，(1,1）指派，¬ $P\vee Q$ 均为 **T**。

定义 2.25 公式 C 称为公式 A 的主合取范式，当且仅当：

1．$C\Leftrightarrow A$；

2．C 仅是不同大项的合取式。

下面的定理实际上提供了一种用真值表来求一个公式的主合取范式的方法。

定理 2.9　一个可满足的公式 A（非永真的）的主合取范式是若干大项的合取式，这些大项的编码恰与全体使得公式 A 为假的指派一一对应相等。

证明　设 $M'_1, M'_2, \cdots, M'_k$ 是使 A 为假的个个不同的全部大项。记 $C = M'_1 \wedge M'_2 \wedge, \cdots, \wedge M'_k$。要证 C 是 A 的主合取范式。

显然这只要证明 $C \Leftrightarrow A$ 就好了。事实上，由这里的假设，用上述 k 个大项中任一个的编码对应的一组真值指派 C 时，C 中恰有一个大项为假（该大项有与指派所用一组真值对应的编码，而其他 k-1 个大项此时为真），所以 C 为假。若以某一组真值指派公式 A，A 为真，按定理假设，与此指派对应的大项必不出现在公式 C 中，于是 $M'_1, M'_2, \cdots, M'_k$ 均为真，所以 C 为真。

定理 2.9 实际上证实了一个非永真的可满足公式的主合取范式是唯一的。

【例 2.30】　写出 $P \rightarrow Q$ 的主合取范式。

解　该公式的真值表最早在 2.2 节中给出（表 2.5）。它在指派（1，0）时为 **F**，所以其主合取范式为 M_{10}，即，其主合取范式是

$$\neg P \vee Q$$

以上主合取范式看上去是一个析取式，其实应当把它看成是只含一个大项的合取式。

【例 2.31】　给出$\neg(P \rightleftarrows Q)$的主合取范式。

解　参阅本章 2.2 中表 2.8。有

$$\neg (P \rightleftarrows Q) \Leftrightarrow (P \vee Q) \wedge (\neg P \vee \neg Q)$$

这就是$\neg (P \rightleftarrows Q)$的主合取范式。

下面就让我们进入如何用不断寻求一个公式的等价公式而最终求得主合取范式的讨论。当然，每一次等价变换，都要使变换后的公式更加接近主范式。

下面是用等价变换的方法求主合取范式的规则：

1. 用等价式 $P \rightleftarrows Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$和表 2.14 中式（11）化去公式中所有条件和双条件联结词。

2. 反复利用表 2.14 中式（7）（摩根律）将否定联结词直接作用到原子变元上。

3. 反复利用表 2.14 中的析取对合取的分配律，直至公式成为若干初等和的合取式。

4. 所得合取式如是主合取范式则结束，否则，考察所有初等和，删去同时含有某一变元及其否定的初等和（因为该初等和为真），将初等和中那些多次出现的同一变元或同一变元的否定均分别合并成一个变元或一个变元之否定，并且合并完全相同的初等和。

5. 若此时已得主合取范式则结束，否则，对不是大项的初等和，若变元 P_d 和$\neg P_d$ 均不存在于初等和中，将此初等和与（$\neg P_d \wedge P_d$)进行析取，再利用析取对合取的分配律化成两个初等和。若需要，合并相同的初等和。返回第 5 步继续。

现在再回到本节开始时的那些话上去，是不是会有一些新的体会呢？

2.7　命题演算的推理理论

有效推理是按照一组严格定义的规则，从一组作为**前提**的命题推导出一个新命题的过程。所得新命题称为是前提的**有效结论**。由于数理逻辑使用自己定义的形式语言，它与所论证的内容无关。它只关心命题的真值之间的关系。所以，我们可以说的只是当前提中的每一命题

均为真时（不一定要求永真），从有效推理得到的结论是一个真命题（同样也不是永真的）。有效推理可以得出假命题，因为只要前提之一为假时，就可能出现此现象。换句话说，有效推理只保证推理本身的合理性，至于前提是否真，将交给推理者去把握。

2.7.1 有效推理的概念

定义 2.26 设 $H_1,H_2,\cdots,H_n$ 和 C 都是 wff。若前者共同蕴含 C，也即

$$H_1 \wedge H_2 \wedge \cdots \wedge H_n \Rightarrow C \tag{2.1}$$

成立，则我们说 C 是这 n 个前提的**有效结论**，或者说 $H_1,H_2,\cdots,H_n$ 可有效推理出 C。通常也记为

$$H_1,H_2,\cdots,H_n \Rightarrow C \tag{2.2}$$

常用推理有多种方法，但每一种都必须符合式（2.1）。

2.7.2 有效推理的方法

有效推理的方法主要有分析法和演绎证明两种，本小节主要介绍演绎证明。

分析法实际上在 2.5.2 中已经提到过。此处仅举一例说明。

【例 2.32】 试证明 $P \wedge Q$ 的有效结论是 Q。

证明

设 $P \wedge Q$ 为真。于是 P 为真，且 Q 为真。Q 为真，即是有效结论。

下面介绍演绎证明。演绎证明又可分为直接证明、条件证明和间接证明。

1．直接证明

直接证明就是构造一个命题公式的序列，使该序列的每一个公式或者就是前提之一，或者是一个被序列中位于其先的一个或若干公式所蕴含。而序列中最后一个公式正是要证的有效结论。

构造以上序列的过程，就是推理的过程。本质上可以这样理解，当保证前提中每一个公式为真时，序列中任一公式亦为真。

为保证引入的公式为真，必须遵循以下的**引入规则**。

（1）**规则 P**：一个前提，可以在推理的任何一步上引入序列。

（2）**规则 T**：一个公式 B，若被推理过程中已得出的若干公式所蕴含，则 B 可被引入论证。

引用 T 规则时当然要遵从表 2.15 和表 2.14 中列出的诸式。为更加符合推理的习惯，我们将表 2.15 的形式适当地做些变更，表中前件在那里是以合取式的形式出现的，现在把这个合取式改写成若干独立的公式序列（类似式（2.2））。例如，对于蕴含式（10'）

$$(P \rightarrow Q) \wedge (Q \rightarrow R) \Rightarrow P \rightarrow R$$

我们写成

$$P \rightarrow Q,\ Q \rightarrow R \Rightarrow P \rightarrow R$$

这样做的好处在于当构造推理的序列时，我们可以引入一个合取式前提的一个合取项。而这样做的理由是显然的，因为，假设一个前提包含若干子前提（子前提的合取式），并且它为真，那么作为它的每一合取项（子前提之一）必为真。

【例 2.33】 证明 $R \vee S$ 是前提 $\neg P \rightarrow (\neg R \rightarrow S)$，$P \rightarrow Q$ 和 $\neg Q$ 的有效结论。

证明

（1）$\neg Q$　　P；

（2）$P\rightarrow Q$　　P；

（3）$\neg P$　　T；（1），（2）

（4）$\neg P\rightarrow(\neg R\rightarrow S)$　　P；

（5）$\neg R\rightarrow S$　　T；（3），（4）

（6）$R\vee S$　　T；（5）

【例 2.34】　试证由前提$(U\vee V)\rightarrow(M\wedge N)$, $U\vee P$, $P\rightarrow(Q\vee S)$, $\neg Q\wedge\neg S$ 可有效推出 M。

证明

（1）$\neg Q\wedge\neg S$　　P；

（2）$\neg(Q\vee S)$　　T；（1）

（3）$P\rightarrow(Q\vee S)$　　P；

（4）$\neg P$　　T；（2），（3）

（5）$U\vee P$　　P；

（6）U　　T；（4），（5）

（7）$U\vee V$　　T；（6）

（8）$(U\vee V)\rightarrow(M\wedge N)$　　P；

（9）$M\wedge N$　　T；（7），（8）

（10）M　　T；（9）

2．条件证明

当要证的有效结论是一个类似 $P\rightarrow Q$ 这样的条件命题时，我们可以将条件命题的前件 P 作为一个**附加前提**，只要该附加前提与原来的前提共同可有效推出原来要证结论 $P\rightarrow Q$ 的后件 Q，那么原始论证必有效（$P\rightarrow Q$ 是有效结论）。事实上，如果原先的一组前提的合取表示成 $H=H_1\wedge H_2\wedge\cdots\wedge H_n$，即要证 $H\Rightarrow P\rightarrow Q$，也即 $H\rightarrow(P\rightarrow Q)$ 为永真，由于有等价关系 $H\rightarrow(P\rightarrow Q)\Leftrightarrow(H\wedge P)\rightarrow Q$（见 2.5 节例 2.21），所以，当 $H\wedge P\Rightarrow Q$，必有 $H\Rightarrow P\rightarrow Q$。这就是所谓条件证明。

上述引入附加前提的规则是所谓 *CP* 规则。

规则 *CP*：当待证明的一个有效结论的形式是条件命题 $P\rightarrow Q$ 时，可将此公式的前件单独提取出来作为一个附加前提，然后证明原来的前提和这个附加前提一道，可有效推出 Q。

【例 2.35】　试证 $P\rightarrow(Q\rightarrow R)$, Q, $P\vee\neg S$ 可有效推出 $S\rightarrow R$。

证明

（1）S　　*CP*；

（2）$P\vee\neg S$　　P；

（3）P　　T；（1），（2）

（4）$P\rightarrow(Q\rightarrow R)$　　P；

（5）$Q\rightarrow R$　　T；（3），（4）

（6）Q　　P；

（7）R　　T；（5），（6）

（8）$S \rightarrow R$　　CP；

3．间接证明

间接证明也称反证法。

定义 2.27　一组前提 $H_1,H_2,\cdots,H_n$ 称为**相容**的，就是说有一个（至少有一个）对前提的真值指派，使得每一前提均为真。一组前提是**不相容**的，就是说对任何一个真值指派，总有一个前提为假。即一组不相容的前提 $H_1,H_2,\cdots,H_n$ 蕴含（更严格地说，是等价于）一个永假式。

$$H_1 \wedge H_2 \wedge \cdots \wedge H_n \Rightarrow R \wedge \neg R$$

其中 R 是任一个合式公式。因为 $R \wedge \neg R$ 是永假式，所以 $H_1 \wedge H_2 \wedge \cdots \wedge H_n$ 是永假的。

为要证明 C 是前提 $H_1,H_2,\cdots,H_n$ 的有效结论，可将否定的结论 $\neg C$ 作为附加前提添加到原来的前提中去，若能证得 $H_1,H_2,\cdots,H_n,\neg C$ 是不相容的，则原推理也同时成立（即 C 是有效结论）。事实上，因为 $H_1 \wedge H_2 \wedge \cdots \wedge H_n \wedge \neg C$ 是永假的，所以，若 $H_1 \wedge H_2 \wedge \cdots \wedge H_n$ 为真时，$\neg C$ 必为假，即 C 为真。

【例 2.36】　试证明 $\neg(P \wedge Q)$ 可由 $\neg P \wedge \neg Q$ 有效推出。

证明

（1）$\neg \neg(P \wedge Q)$　　P；（附加前提）
（2）$P \wedge Q$　　T；（1）
（3）P　　T；（2）
（4）$\neg P \wedge \neg Q$　　P；
（5）$\neg P$　　T；（4）
（6）$P \wedge \neg P$　　T；（3），（5）

【例 2.37】　试用反证法证明 $W \vee S$ 可由 $S \vee U$, $U \rightarrow (Q \wedge R)$ 和 $Q \rightarrow W$ 有效推出。

证明

（1）$\neg (W \vee S)$　　P；（附加前提）
（2）$\neg W \wedge \neg S$　　T；（1）
（3）$\neg W$　　T；（2）
（4）$Q \rightarrow W$　　P；
（5）$\neg Q$　　T；（3），（4）
（6）$\neg S$　　T；（2）
（7）$S \vee U$　　P；
（8）U　　T；（6），（7）
（9）$U \rightarrow (Q \wedge R)$　　P；
（10）$Q \wedge R$　　T；（8），（9）
（11）Q　　T；（10）
（12）$Q \wedge \neg Q$　　T；（5），（11）

【例 2.38】　试给出以下推理。

一个科室选定出差的人。要求满足以下条件：

如果李去，则王必须去。

张和王不能同时去。

结果是：如果张去，则李不能去。

证明

先将前提和结论写成形式语言。

设 Z：张去。L：李去。W：王去。于是要证 $L \rightarrow W$, $\neg(Z \wedge W)$有效推出 $Z \rightarrow \neg L$。

（1）$\neg(Z \rightarrow \neg L)$　　P；（附加前提）

（2）Z　　T；（1）

（3）$\neg (Z \wedge W)$　　P；

（4）$\neg Z \vee \neg W$　　T；（3）

（5）$\neg W$　　T；（2），（4）

（6）$L \rightarrow W$　　P；

（7）$\neg L$　　T；（5），（6）

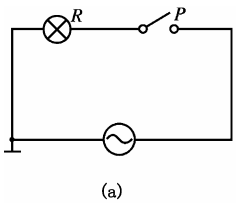
（8）L　　T；（1）

（9）$L \wedge \neg L$　　T；（7），（8）

2.8　命题逻辑和二值逻辑器件

至今我们讨论的命题逻辑叫做**二值逻辑**，因为在这里每一个命题可能取到的逻辑值只有“T”和“F”（或“1”和“0”）两个。各种工程技术中常用的一些机械或电子器件，也存在类似的情况。例如一个开关或继电器通常存在一些成对的触点，它们或处于闭合状态（以“1”表示之），或处于断开状态（以“0”表示之）。所以它们被称为**二值器件**。

开关或继电器通常用来控制某些器械的工作状态。例如图 2.1（a）给出了日常生活中的照明线路，当接于线路中的开关断开时，电路中的电灯就不工作（熄灭），而当开关闭合时，电灯就工作（点亮）。若将电灯的“亮”和“灭”分别以“1”和“0”来表示的话，可将电灯的状态 R 和开关的状态 P 之间的逻辑关系表达为 $R \Leftrightarrow P$。图 2.1（b）给出了它们的**组合表**（也可称为真值表）。



(a)

P	R
0	0
1	1

(b)

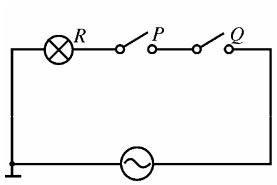
图 2.1　开关控制电灯的例子

图 2.2（a）给出了两只串联开关控制一只电灯的例子。如果分别以 P,Q 以及 R 表示两只开关以及电灯的状态的话，图 2.2（b）就是它们的组合表。由表中不难看出关系式 $P \wedge Q \Leftrightarrow R$ 成立。就是说，串联的开关电路对应着逻辑上的一个合取式。自然容易想到，两只并联的开关将对应着一个析取式，图 2.3 给出了这个电路和与之对应的组合表。

在以上的讨论中，我们把开关的状态称为输入变量，电灯的状态称为输出变量。而一个有效的电路（由一些二值器件和工作器件组成）正是建立了一种输出变量与输入变量之间确定的关系。

通常的逻辑电路主要是由一些称为“门”的电子器件组成的。在这类电路中，输入变量和输出变量都只具有高电位和低电位两种状态，我们分别以“1”和“0”来表示其逻辑值。

习惯上，用一个符号框图来表示一个门电路。为了沿用逻辑电路中约定的符号，本节以下的部分分别用状态变量上加“ ¯ ”表示“┐”（例如┐ P 写成 $\overline{P}$ ），而用“·”和“+”分别表示“∧”和“∨”。

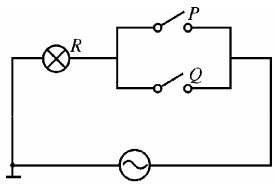


(a)

P	Q	R
0	0	0
0	1	0
1	0	0
1	1	1

(b)

图 2.2　串联开关的例子



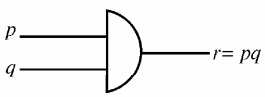
(a)

P	Q	R
0	0	0
0	1	1
1	0	1
1	1	1

(b)

图 2.3　并联开关的例子

图 2.4（a）和图 2.4（b）分别给出了**与门**的框图符号和输入 p,q 与输出 r 的关系。



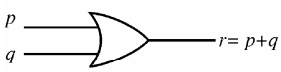
(a)

p	q	r
0	0	0
0	1	0
1	0	0
1	1	1

(b)

图 2.4　与门的框图和组合表

图 2.5（a）和图 2.5（b）给出了**或门**的框图和对应的组合表。



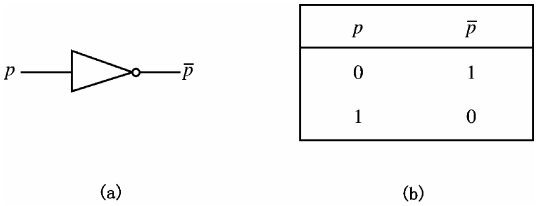
(a)

p	q	r
0	0	0
0	1	1
1	0	1
1	1	1

(b)

图 2.5　或门的框图和组合表

图 2.6（a）和图 2.6（b）是**非门**（反相器）的框图和组合表。



p	$\bar{p}$
0	1
1	0

图 2.6　非门的框图和组合表

用与门、或门以及非门这三种基本的器件，就可组成与任一逻辑表达式对应的逻辑电路（参考 2.2.2 小节，理论上讲，只要有非门以及与门、或门两者之一就够了）。例如图 2.7 中，图 2.7（a）表示一个对应着逻辑公式$(P\vee Q)\wedge R$，即$((p+q)\cdot r)$的电路；图 2.7（c）表示一个对应于逻辑公式 $P\wedge\neg Q$，即$(p\cdot\bar{q})$的逻辑电路（注意到这就是$\neg(P\rightarrow Q)$的电路）；而图 2.7（b）对应于逻辑表达式$(\neg P\wedge Q)\vee(P\wedge\neg Q)$，即$((\bar{q}\cdot q)+(p\cdot\bar{q}))$，也即与一个异或电路$(P\overline{\vee}Q)$等价。

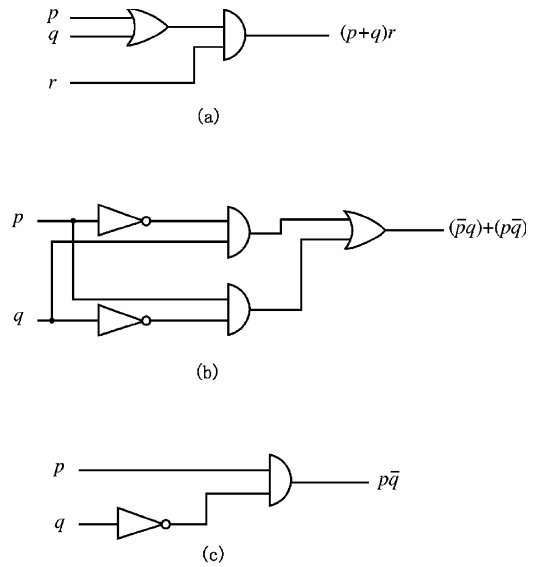


图 2.7　与逻辑表达式对应的逻辑电路

实际使用的门电路，其输入端可增加至多于 2 个。另外也还有将与门和非门或者是或门和非门构成一个组件的情况，这就是所谓的“与非门”或者“或非门”。

一般来说，在一个由门组成的电子电路中，从输入信号稳定地建立起，至输出信号稳定地建立为止，有一段延迟时间。经过一个反相器、与门和或门的延迟时间通常称为一级标准门延迟。一个组合电路的延迟是一条从输入端至输出端的最长的路径上通过的门的延迟时间之和。例如图 2.7 中的（a），（b），（c）的延迟时间分别为 2,3,2 级门延迟。显然延迟时间越短越好。为要减少延迟时间，就需要用一个与之等价但延迟级数较少的电路去替代它。而命题逻辑中关于公式的等价变换,在此可以派上用场。

例如，设计一个由三方参与的表决机器，规则是简单的“少数服从多数”。我们以 C_1,C_2,C_3 表示参与表决的三方的输入。“1”表示同意，“0”表示反对。以 S 表示表决的输出结果。“1”表示通过，“0”表示未通过。可以写出 S 的逻辑表达式的主析取范式形式如下：

$$S\Leftrightarrow(\neg C_1\wedge C_2\wedge C_3)\vee(C_1\wedge\neg C_2\wedge C_3)\vee(C_1\wedge C_2\wedge\neg C_3)$$
$$\vee(C_1\wedge C_2\wedge C_3)$$

绘出该表达式对应的逻辑电路，如图 2.8（a）所示。容易看出该电路有 3 级门延迟。现在将上面的主范式化简。

$$S\Leftrightarrow((\neg C_1\wedge C_2\wedge C_3)\vee(C_1\wedge C_2\wedge C_3))\vee$$
$$((C_1\wedge\neg C_2\wedge C_3)\vee(C_1\wedge C_2\wedge C_3))\vee$$
$$((C_1\wedge C_2\wedge\neg C_3)\vee(C_1\wedge C_2\wedge C_3))$$
$$\Leftrightarrow(C_2\wedge C_3)\vee(C_1\wedge C_3)\vee(C_1\wedge C_2)$$

于是 S 的最后这个表达式对应的逻辑电路可表示成图 2.8（b）的形式。显然，这组电路只有 2 级门延迟。速度提高了 30%多。

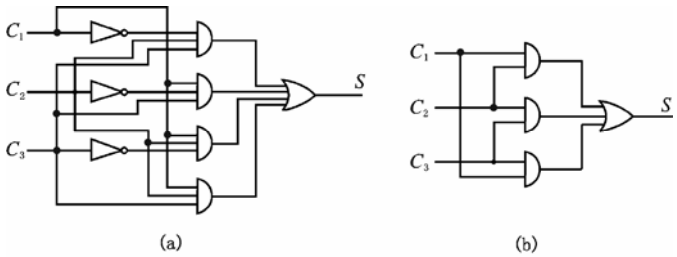


图 2.8　表决机器的逻辑电路

关于电路的化简，在第 7 章中还会专门讨论。

最后，我们通过两个例子来看一看命题逻辑的知识在逻辑电路设计上的应用。

【例 2.39】　楼梯间安有一盏电灯，在楼上与楼下各安装一只开关。请设计一个电路，要求无论当前电灯是点亮的还是熄灭的，只要拨动这两只开关的任意一只，就可改变电灯的当前状态。

解　设电灯的状态用 S 表示，并令“0”代表熄灭状态，“1”表示点亮状态。两只开关的状态分别以 K_1 和 K_2 表示。“0”表示拨杆的某一位置（如向上），“1”表示其另一位置。我们可以这样分析，设当前电灯是 $S=0$ 状态，K_1 和 K_2 也均为 0 状态。无论拨动两只开关中哪一只，电灯状态变为 $S=1$。不妨设，改变 $K_2=1$。下一次再拨动两只开关中的一个，若这回拨动的是 K_1，则 $K_1=1$，而 K_2 仍保持原状态 $K_2=1$，此时电灯应改变为熄灭状态 $S=0$；若第二次拨动的仍是 K_2，则电灯及开关的状态回到原始状态。如果从初始状态开始，首先拨动的是 K_1，情况完全同以上讨论相似。据此可以列出电灯与开关的状态的组合表（见表 2.16）。从表上可知，逻辑变量 S 是 K_1 和 K_2 的异或。

表 2.16　电灯与开关的组合表

K_1	K_2	S
0	0	0
0	1	1
1	0	1
1	1	0

即

$$S\Leftrightarrow K_1\overline{\vee}K_2\Leftrightarrow\neg K_1\rightleftarrows K_2$$

所以绘出的逻辑框图与图 2.7（b）完全相同，只是将那里的输入端换成 K_1 和 K_2，输出端就是所要的状态 S。

要用手控的机械开关组成这个电路，需要用一种一般称为双联开关的电器。它上面有三个接线端子，画出的实际电路如图 2.9 所示。我们注意到，当两开关的状态分别为 0,l 或者 1,0 时，电路被接通，否则电路是断路的。

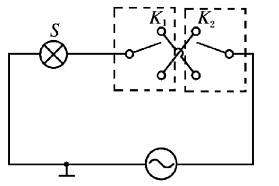


图 2.9　由双联开关接成的异或电路

【例 2.40】　设计一个博物馆的警报系统。要求如下。（a）仅当系统的总电源开关闭合时，系统才可能报警；（b）当总电源开关闭合时，以任何方式打开通向受监控区的主通道门时，主通道门上的传感器动作并使警报系统动作；（c）为便于保卫人员的巡视所设的一个专用休眠开关未合上时，监控区的门户就被打开，这时门户上的传感器动作并报警。

解　首先我们用一些变量表示题中有关的一些语句。

A：警报系统动作。

M：总电源开关闭合。

G：主通道被入侵。

W：监控区的门户打开。

S：休眠开关闭合。

于是变量 A 作为输出，可以表达为如下的形式

$$A \Leftrightarrow M \wedge (G \vee (W \wedge \neg S))$$

习惯上，也可写成

$$a = m \cdot (g + (w \cdot \bar{s}))$$

对应的框图如图 2.10（a）所示。如有需要减小门延迟时间，可将上述表达式写成

$$a = m \cdot g + m \cdot w \cdot \bar{s}$$

对应的框图如图 2.10（b）所示。这样可以减少一级门延迟。如果我们使用由三极输入的与门，电路可以如图 2.10（c）那样。

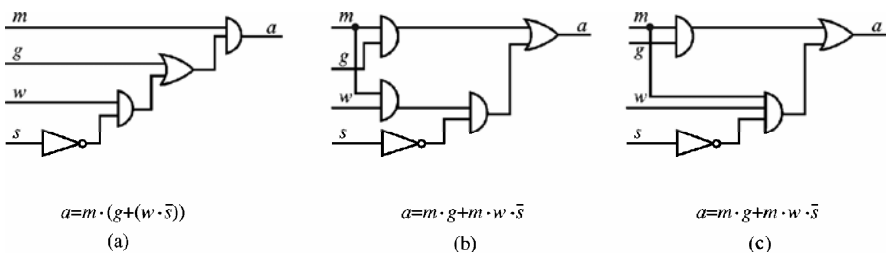


图 2.10　博物馆的报警系统

2.9　一阶谓词逻辑

截止到目前，我们讨论的都是所谓“命题逻辑”的演算。在那里，命题是形式语言中最基本的单位，即完全避免拆分一个原子命题。这样，就产生了一个问题。有些明显是正确的推理，却不可能由命题演算来完成，如

P：每一个人都将死去。

Q：苏格拉底是人。

R：苏格拉底将死去。

无论如何，我们无法用命题逻辑中的推理规则从 P,Q 推出结论 R。

经过分析发现（正是苏格拉底本人给出了上面的例子而且分析了它），将以上三个命题看成是不可分解的做法，掩盖了它们之间某些成分之间的内在联系：或者它们的主语相同或有归属关系，或者它们的谓语一样。这种命题的部分（不再是语句，而只是组成语句的元素）之间的关系，启发了人们将语句进一步拆分成**个体**（或成员对象）和谓词两部分。于是，通过个体或谓词的关系建立起命题之间的逻辑关联。所以，本质上说，谓词逻辑是建立在对命题或命题公式的个体的推理上的逻辑形式。即使这样，命题之间的逻辑关系依然遵循命题逻辑的所有规律。

基于以上的讨论，一种称为**谓词逻辑**的符号逻辑分支被建立了起来。在谓词逻辑里，引入了谓词和个体的概念。

设有这样两个命题：

张三是大学生。

李四是大学生。

如果要在命题逻辑里将它们符号化，那我们不得不用两个不同的标识符，譬如 P 和 Q。可是这两个命题并非完全无关的。事实上它们虽然描述的是两个不同的对象，张三和李四，但该两个对象却有着共同的属性，即“是大学生”。相反，如果我们将这两个语句的每一个都表示成描述的对象和该对象的属性这样两部分的话，这种共同的特征就被显露出来了。

还有些命题描述多于一个个体之间的关系。例如

3 小于 5。

张三比李四高。

王五坐在张三和李四之间。

它们分别包含 2 个、2 个和 3 个对象。

描写对象的属性或其关系的语词，我们称之为谓词。具有与一个个体相联系的谓词称为**一元谓词**，与两个个体联系的谓词称为**二元谓词**，一般地，与 n 个个体联系的谓词称为 ***n* 元谓词**。并约定，一个命题标识符被称为**零元谓词**。谓词通常用大写字母表示，而个体则用小写字母表示。在谓词逻辑里，一个完整的原子命题由一个确定的谓词符号和紧跟其后的一个或多个个体符号来表示。所有个体用圆括号括起来。如果有多于一个个体，则两个体间以“,”号分隔。

下面是将一命题在谓词逻辑下符号化的例子。

【例 2.41】 分别将以下命题用谓词的形式符号化。

（1）张三是大学生。

（2）李四是大学生。

（3）张三与李四是同学。

（4）王五坐在张三和李四中间。

解

首先令

z：张三，l：李四，w：王五

S：是大学生，C：是同学

I：××坐在××与××之间

于是，符号化以后有：

（1）$S(z)$

（2）$S(l)$

（3）$C(z,l)$

（4）$I(w,z,l)$

特别注意当 $n>1$ 时，n 元谓词之后的诸个体的次序是重要的。例如上例中若写出 $I(z,w,l)$ 则表示的是“张三坐在王五和李四之间”。如果谓词是在描述诸个体空间位置或其某种逻辑次序的话，不可将这种实际上的空间位置及次序与谓词中表达诸个体时的先后次序相混淆。

2.10 命题函数和个体变量及量词

有一些语句表示不同个体的同一属性或其间的同一关系。例如，“上海是国际大都市”、“纽约是国际大都市”等，或者“火车比汽车快”、“飞机比火车快”等。前两个语句分别表示两个不同城市都是国际大都市，而后两个语句则分别表示两组不同的交通工具中，每一组的前者比后者更快捷。如果我们以 $C(x)$ 表示“x 是国际大都市”，$F(x,y)$ 表示“x 比 y 快”，那么，所有希望表示“某某是国际大都市”的语句都有一样的形式，就是 $C(x)$。对 $F(x,y)$ 也有类似的情况。在这里，x 或 y 并不代表某一具体的对象，它好似代数表达式 $u+3uv+v$ 那样，其中的 u 或 v 只是一个字母，并不真是一个实数，但是当用任何两个实数分别替代 u 和 v 之后，该代数表达式可得出一实数值。在我们这里，类似地，小写字母 x ,y 只是为事后将要取代它的某些真实的对象“占据一个位置”，换句话说，这些字母的存在，只是表达了这样一层意思：在这些字母存在的地方，将可以用任一确定的对象名字来代替它。像这一类小写字母，我们称之为**个体变量**，简称为**变量**或**变元**。包含个体变量的谓词表达式称为**简单命题函数**或**原子命题函数**。以上 $C(x)$ 和 $F(x,y)$ 都是原子命题函数。

2.10.1 命题函数

命题函数本身并不是命题，因为它不含具体的个体，所以命题函数无所谓真或假。可是一旦以适当数量的具体对象名逐一替代命题函数中所有的变量之后，命题函数就成了一个有明确真假值的命题了。回到一开始的例子，$C(x)$ 是命题函数。当以 s（上海）替代变量 x 后，$C(s)$ 就表示“上海是国际大都市”这个真命题了。假若以 f 表示《复活》这本书，那么 $C(f)$ 就是假的命题。

这里讨论的是如何使一个命题函数转化成一个命题的一种初等方法。还有一种更重要的方法，就是通过使用量词对变量产生必要的约束来实现的。稍后再来讨论它。

使用联结词（命题演算中给出过五种主要联结词）可以恰当地将一些原子命题函数联结成复合命题函数。下面是一些例子。

设 $M(x)$：x 是人。

$A(x)$：x 是动物。

$M(x)\wedge A(x)$：x 是人且 x 是动物。

$\neg A(x)$：x 不是动物。

$M(x)\rightarrow A(x)$：如果 x 是人，那么 x 是动物。

必须指出，一个命题函数中的变量换用另一些字母来表示时，并不会改变该命题函数本身。譬如以 u 和 v 分别取代 $F(x,y)$中的 x 和 y，得到的 $F(u,v)$本质上与 $F(x,y)$并无区别。记住上面我们说过的话：这些变量只是为事后将取代它们的具体个体占据一个位置。

2.10.2 量词

谓词逻辑涉及个体，有很多论证不只是对某些具体的个体进行的，这些论述时常涉及一整类个体或一整类个体中不特别指明的某一个。例如，“所有的人都是动物”、“有些人是左撇子”等。显然，对前一个语句，无论你用 $M(x)$或 $A(x)$甚至 $M(x)\rightarrow A(x)$都无法表示它。请记住，最后这三种表达式只是三个命题函数，根本不是命题，它们并无真假值。而“所有人都是动物”却确实是一个真命题。

在谓词逻辑中引入所谓**量词**之后，就可以解决上述问题。量词是谓词逻辑确切定义的一种语素，它是一种短语。量词分全称量词和存在量词两种。

全称量词 记号(x)或$(\forall x)$，读做“所有的 x”。它由全称量词的符号“$\forall$”和被该量词限定的变量 x 两部分组成。通常用括号将它们联系在一起。

存在量词 记号$(\exists x)$，读做“有一个（至少一个）x”。它也是由量词符号“$\exists$”和被限定的变量 x 组成。

约定，将一个量词放在一个命题函数之前。例如$(\forall x)M(x)$和$(\exists x)S(x)$。这样一来，命题函数中的变量均已被该量词所限定。翻译成自然语言，就是

$(\forall x)M(x)$：所有的个体都是人。

$(\exists x)S(x)$：有一个（至少有一个）个体是大学生。

很显然，还必须为我们正在议论的对象（如这里的 x）指明一个范围，如果对于表达式$(\forall x)M(x)$考虑的个体的集合是宇宙中的所有事物，也即量词是对于宇宙万物这个范围限定的，那么它是一个假语句。若指明是在地球上各种族的全体人类的范围内来考察表达式的话，则$(\forall x)M(x)$就是一个真的命题了。很容易看出，被妥善限定的命题函数已经转化成一个命题。虽然该命题的真值随着我们讨论的个体的集合有所变化，不过一般情况下，在每一个论证中，不难从上下文找到这一论证所规定的个体的集合。这种对于每一次特定的讨论中，事先约定的关于所讨论的个体的集合，称为**论域**或**个体域**。如果不事先指明论域，我们将认为论域是一切可以作为对象的东西的集合，这时，称讨论是在**全总论域**下进行。全总论域也称**全总个体域**。

对于多元谓词构成的命题函数也有类似的情况。设 $P(x,y)$是一个二元词谓词，它表示“x 与 y 是 P”。若对于它的所有这两个变量分别予以限定，可以有以下四种情况：

$(\forall x)(\forall y)P(x,y)$：所有的 x 中的每一个与所有的 y 中的每一个是 P。

$(\exists x)(\forall y)P(x,y)$：有一个 x 与所有 y 中的每一个是 P。

$(\forall x)(\exists y)P(x,y)$：所有 x 的每一个与有一个 y 是 P。

$(\exists x)(\exists y)P(x,y)$：有一个 x 与有一个 y 是 P。

以上这四种情况中，每一种都得到一个命题。

为使用多个量词时不产生歧义，我们约定：多个量词连续出现在一处时，遵循左结合运算，即按从右至左的方向解释，首先将最右边一个量词与右边谓词表达式结合起来，然后依次从右至左地把每一量词作用于它的右边的表达式。

例如$(\forall x)(\exists y)P(x,y)$ 理解为$(\forall x)((\exists y)P(x,y))$。在上述左结合的约定下，$(\exists y)P(x,y)$外面的括号可以省去。于是$(\forall x)(\exists y)P(x,y)$的含义是：每一个个体 x，它和某一个个体 y 是 P，而$(\exists y)(\forall x)P(x,y)$的意思是有一个个体 y 和任何一个 x 是 P。请留意它们是不同的命题。因为后一命题表示存在一个确定的 y，它和任何 x 都是 P；而前者虽表示每一个 x（$x_1,x_2,\cdots$）都和一个 y 是 P，但可能 x_1 与 y_1 是 P，x_2 与 y_2 是 P，但是当 $x_1 \neq x_2$，则 $y_1 \neq y_2$。

综上所述，在确定的论域下，对一个命题函数中的每一个变量均用一个量词加以限定，则该命题函数转化为一个命题。

这就是上文中提到的使一个命题函数转化成命题的另一方法。

2.11 谓词公式

2.11.1 谓词公式

类似于命题演算中的合式公式概念，**谓词逻辑演算**中有严格定义的**谓词表达式**，即所谓**合式的谓词公式**。

首先让我们来规定谓词公式涉及的四类符号：

1.（个体）常量符号：用小写字母 a,b,c 等表示。在给定的个体域 D 下，它们是属于 D 中的某一个确定的个体。可表示成 $a\in D$，$b\in D$，$c\in D$，等等。

2.（个体）变量符号：用小写字母 x,y,z 等表示。在给定的个体域 D 下，它们可以被任何一个属于 D 的（个体）常量（即确定的个体）所替代。

3.（个体）函数符号：用小写字母 f,g,h 等表示。它们是定义在个体域 D 上的 n 元函数 f（$x_1,x_2,\cdots,x_n$），且函数的值域包也是一个个体域。

4．谓词符号：用大写字母 P,Q,R 等表示。在给定个体域 D 下，符号 $P(x_1,x_2,\cdots,x_n)$必须是任何一个确定的 n 元谓词。

以上四种符号，前三种是关于个体的，统称为**项**。最后一种是关于谓词的。在这里，我们约定不含任何个体列表的谓词符号，如 P，则表示一个命题变元。前面提到过，它是零元谓词，取其不显含个体变元之义。

给一个关于个体函数的例子。

设 W 表示全世界女子足球队的集合，用 L 表示所有女足队长的集合。定义 W 上的函数 $f(x)$，它的值是 x（某女足）的队长。$f(x)$的值域就是 L。另设谓词 $F(x)$表示 x 是当今世界最优秀球星。$w\in W$，w 表示中国女足。则 $F(f(w))$表示语句“中国女足的队长是世界最优秀的球星”。

应当着重指出的是：在一阶谓词演算中，谓词符号不是变量，而是事先任意确定的一个谓词。所以量词不能作用在谓词上。如$(\forall P)P(x)$就不属于一阶谓词演算讨论之列。一阶谓词逻辑也称**狭义逻辑**。

定义 2.28　一阶谓词中的项，递归地定义如下：

1．常量符号是项。

2．变量符号是项。

3．若 $f(x_1,x_2,\cdots,x_n)$是 n 元函数，$t_1, t_2, \cdots, t_n$ 都是项，则 $f(t_1, t_2, \cdots, t_n)$也是项。

4．只有可有限次利用以上 1,2,3 各个步骤生成的符号串是项。

定义 2.29　一阶谓词中，若 $P(x_1,x_2,\cdots,x_n)$是 n 元谓词，$t_1,t_2,\cdots,t_n$ 都是项，那么 $P(t_1,t_2,\cdots,t_n)$是**原子命题函数**。

例如 $P(x,y)$, $Q(x,f(x))$, $R(a,x,y)$都是原子命题函数。特别是作为命题逻辑中的原子命题变元（零元谓词），如“S”，取代它的必须是某一个确定的命题。

定义 2.30　合式谓词公式递归定义如下：

1．原子命题函数是合式的。

2．若 A 是合式的，$\neg A$ 也是合式的。

3．若 A,B 是合式的，$(A\wedge B),(A\vee B),(A\rightarrow B),(A\rightleftarrows B)$都是合式的。

4．若 x 是出现在合式公式 A 中的个体变量，则$(\forall x)A,(\exists x)A$ 都是合式的。

5．只有可有限次利用以上 1,2,3,4 各个步骤生成的符号串是合式的。

与命题演算类似，约定，整个合式的谓词公式最外层的括号可以省略。

现在来讨论如何用谓词公式将以下两个语句符号化。

（1）所有的人都是动物。

（2）有一些人是左撇子。

显然，这两个语句都是真的。为了准确地翻译它们，将这两个语句改写一下：

（1a）对于个体域 D 中的每一个对象 x，如果 x 是人，则 x 是动物。

（2a）在个体域 D 中，至少有一个对象 x，x 是人而且 x 是左撇子。

于是（1），（2）两个语句可以正确地翻译成：

（1b）$(\forall x)(M(x)\rightarrow A(x))$

（2b）$(\exists x)(M(x)\wedge L(x))$

上面出现的谓词，分别定义为 $M(x)$：x 是人；$A(x)$：x 是动物；$L(x)$：x 是左撇子。

我们要特别指出，今后凡要表达形式如“所有是 P 的对象，都是 Q”或者“所有 x，若 x 是 P 则 x 是 Q”这样的语句，必须使用条件联结词，使之符号化为$(\forall x)(P(x)\rightarrow Q(x))$，例如上面的语句（1b）。这样，确保它在任何个体域下都是正确的。如果以任何确定的个体 $a\in D$ 代入$(M(x)\rightarrow A(x))$中，当 a 是某人，则 $M(a),A(a)$都真，从而 $M(a)\rightarrow A(a)$亦真；当 a 不是一个人，则 $M(a)$为假，可是 $M(a)\rightarrow A(a)$仍是真的。如不正确地以合取代替条件联结词，将语句（1）表示成$(\forall x)(M(x)\wedge A(x))$，当 a 不是一个人时，它就是假的了。因为此时若 $a\in D$ 不是一个人，则 $M(a)\wedge A(a)$为假，就不能保证该语句在个体域 D 上是真的了。明白这一点后，我们可以推知（本节稍后将给出），要将形式如“有一个是 P 的对象，它是 Q”这样的语句符号化时，正确选用的联结词应当是合取，即$(\exists x)(P(x)\wedge Q(x))$。

我们以一些语句符号化的例子来结束本节。

在下列例题中，如不特别说明，都是在全总个体域下进行的。

【例 2.42】　人无完人。

解　首先将原语句改变成“所有人都是有缺点的”，并令

$M(x)$：x 是人，$B(x)$：x 有缺点。

于是有

$(\forall x)(M(x)\rightarrow B(x))$

【例 2.43】　实数不必是有理数。

解　令 $R(x)$：x 是实数，$Q(x)$：x 是有理数。

我们可以改变原句使之便于符号化，即“不是所有的实数都是有理数”。于是符号化为

$\neg(\forall x)(R(x)\rightarrow Q(x))$

【例 2.44】 将序列 S_n 的极限 $\lim\limits_{n\to+\infty} S_n = S$ 的定义符号化。

解 $\lim\limits_{n\to+\infty} S_n = S$ 可描述为：对于任意给定的正实数 $\varepsilon>0$，都有正整数 N，使得当 $n>N$ 时就有 $|S_n - S|<\varepsilon$。

令 $R(x)$：x 是实数，$Z(x)$：x 是整数

$G(x,y)$：x 大于 y，$b(x,y)=|x-y|$（这是一函数）

于是符号化后的极限定义可表示为

$$(\forall\varepsilon)\{(R(\varepsilon)\wedge G(\varepsilon,0))\rightarrow(\exists N)[Z(N)\wedge G(N,0)\wedge(\forall n)((Z(n)\wedge G(n,N))\rightarrow G(\varepsilon,b(S_n,S)))]\}$$

上述谓词公式也可等价地表示为

$$(\forall\varepsilon)(\exists N)(\forall n)\{(R(\varepsilon)\wedge G(\varepsilon,0))\rightarrow[Z(N)\wedge G(N,0)\wedge(Z(n)\wedge G(n,N))\rightarrow G(\varepsilon,b(S_n,S)))]\}$$

为了清晰地表达上述两个表达式的层次结构，除圆括号以外，我们还用了方括号和花括号。最后，只要将这两个公式中的后两种括号相应地都换成圆括号后，就是我们需要的合式公式。

2.11.2 变量的约束和替换

量词短语是由量词符号“∀”或“∃”和紧跟其后的被限定变量（如 x,y 等）组成的。量词短语通常用括号加以界定，可简称为量词。量词之后紧接着的第一个公式叫做该量词的**辖域**。这里所说的“紧跟其后的公式”是指从量词之后的第一个符号开始连续向右，直至首次出现的一个完整的合式公式为止的部分。例如

（1）$(\forall u)(P(u)\rightarrow Q(u))$

（2）$(\forall x)P(x,y)$

（3）$(\exists x)P(x)\rightarrow(\forall y)(\exists z)(Q(x,y)\wedge R(z))$

上面（1）中的量词$(\forall u)$的辖域为$(P(u)\rightarrow Q(u))$，（2）中的量词$(\forall x)$的辖域是 $P(x,y)$，（3）中的量词$(\exists x)$的辖域是 $P(x)$（它不包含 $Q(x,y)$），$(\exists z)$的辖域是$(Q(x,y)\wedge R(z))$，而$(\forall y)$的辖域是$(\exists z)(Q(x,y)\wedge R(z))$。

一个谓词公式中的变量出现在某一量词的辖域中，并且它与该量词中的限定变元相同时，称该变量是在公式中的**约束出现**，同时，约束出现的变量称为**约束变量**。公式中其他非约束出现的变量称为**自由变量**。例如在上面公式（3）中，$P(x)$中的 x 是约束出现，而 $Q(x,y)$中的 x 是自由出现。由于从公式的结构上看去，它们的区别是明显的。所以即使这两个性质完全不同的变量选用了同一个符号，也不致引起混淆。不过，当一个公式相当复杂时，用同一个符号既代表一个约束变量，同时又代表另一个自由变量，多少总会带来一些混淆。为了避免这种情况的出现，我们可以将同名的约束变量和自由变量两者之一换用一个新的名字，这就是下面要给出的约束变量和自由变量换名的规则。

首先，本章 2.10.1 小节的最后已经指出，一个谓词公式中的变量用什么字母为它命名是无所谓的。在引入了量词之后，只要我们将量词中的被限定变量和它的辖域中的所有与之同名的约束变量改成同一个新名字，显然也不至于影响这一公式的逻辑意义。例如$(\forall x)P(x)$与$(\forall y)P(y)$就表示的是同一含义：“所有的个体都是 P”。当然，在一个不这么简单的谓词公式中为约束变量换名，就要受到一定的限制。

约束变量的换名规则

1．若要将一约束变量 x 换名，则必须将包含这个约束变量的辖域中所有变量 x 和相应量词短语中的被限定量词 x 都换以同一个新的名字；

2．约束变量换用的新名字，必须与其所在的辖域中的任何一个别的变量名字不同。

例如

$$(\forall x)(\exists y)(P(x,y)\rightarrow Q(z,y))\wedge R(y)$$

正确地对 y 换名可以得到

$$(\forall x)(\exists u)(P(x,u)\rightarrow Q(z,u))\wedge R(y)$$

但是

$$(\forall x)(\exists u)(P(x,u)\rightarrow Q(z,y))\wedge R(y)$$

和

$$(\forall x)(\exists z)(P(x,z)\rightarrow Q(z,z))\wedge R(y)$$

都是不正确的换名。因为前者违背了上述规则 1，使辖域中原本是约束出现的 $Q(z,y)$中的 y 成了自由出现；而后者则违背了规则 2，使原本 $Q(z,y)$中是自由出现的变量 z 变成了约束出现。

自由变量的换名规则

1．若要将公式中的某自由变量 x 以一个新的名字代替，必须将整个公式中所有 x 的自由出现处都代以同一个新名字；

2．用以代替 x 的新名字，必须与公式中所有别的变量（约束的和自由的）都不同名。

例如，有公式

$$(\forall x)P(x,y)\rightarrow((\forall u)Q(u,x)\rightarrow((\exists v)R(v,y)\wedge W(y,x)))$$

为了将公式中自由出现的变量 x 改名，可以用新变量名 z 代替，写成

$$(\forall x)P(x,y)\rightarrow((\forall u)Q(u,z)\rightarrow((\exists v)R(v,y)\wedge W(y,z)))$$

而

$$(\forall x)P(x,y)\rightarrow((\forall u)Q(u,x)\rightarrow((\exists v)R(v,y)\wedge W(y,z)))$$

和

$$(\forall x)\mathrm{P}(z,y)\rightarrow((\forall u)Q(u,z)\rightarrow((\exists v)R(v,y)\wedge \mathrm{W}(y,z)))$$

以及

$$(\forall x)P(x,y)\rightarrow((\forall u)Q(u,u)\rightarrow((\exists v)R(v,y)\wedge W(y,u)))$$

都是不正确的更名。因为前一个没有将 $Q(u,x)$中自由出现的 x 同时换以 z；第二个将原先是约束出现的 $P(x,y)$中的 x 也一起换成了 z；而最后一个换名的错误在于作为新变量名的 u 与公式中的原有的约束变量同名了。

总而言之，无论是对约束变量或者自由变量更换名字，都应记住，换名之后不可改变原公式的结构。说得更明白一点就是，更名以后原先为自由出现的变量还是自由出现的，原先约束出现的变量仍然是约束出现的，并且原先是两个不同的自由（或约束）变量，更名后仍然必须是不同的自由（或约束）变量。遵循这样的普遍原则，可以将

$$(\exists x)P(x,y)\vee Q(u,v)$$

中的自由变量 u 更名为 x，成为

$$(\exists x)P(x,y)\vee Q(x,v)$$

这样的更名，从形式上看 $Q(x,v)$中的变量 x 与$(\exists x)P(x,y)$中的变量 x 同名了，可是由于前者不出现在量词 x 的辖域中，所以本质上来说，仍不改变公式的逻辑结构。因此，我们说，上面给出的自由变量的更名规则 2 是过分严格了些。不过，这样做，使得我们在对变量的更名时更加简便而且不会出错。

2.11.3 谓词演算中的等价与蕴含

合式的谓词公式一般并不是一个命题，因为其中包含有两类“不确定”的因素。其一，是谓词符号和定义于个体域上的函数。其二，是个体变量。前面已经说过，在一阶谓词逻辑里，唯一的变量符号是个体变元。对于第一类符号，我们总是约定它们是事先确定的。至于第二类符号即个体变量，我们有两种方法约束它：（1）用一个确定的个体（如张三、李四……）取代它；（2）用一个量词来限定一个个体变元。

当谓词公式中每一个符号分别按上述规则被设置好以后，我们就可以肯定地说，谓词公式转化为一个有确定真值的命题。在个体域 D 是有限集时，我们甚至可以通过对谓词公式的一个**解释**，来实现上述转化。

在一个恰当的指派下，合式的谓词公式有唯一的真值。以下是关于解释的一个例子。

【例 2.45】 设有谓词公式

（1）$(\exists x)P(a,f(a,x))$

（2）$(\forall x)P(a,f(a,x))$

在个体域 $D=\{a,b\}$ 上，解释如下：

$P(a,a)$	$P(a,b)$	$P(b,a)$	$P(b,b)$
1	1	0	0

$f(a,a)$	$f(a,b)$	$f(b,a)$	$f(b,b)$
a	b	a	b

由于 $x=a$, $f(a,a)=a$，则 $P(a,f(a,a))=P(a,a)=1$。所以，不必再讨论 $x=b$ 的情况即可断言 $(\exists x)P(a,f(a,x))$ 有真值 1。

对于公式（2），$x=a$ 时情况同上。令 $x=b$, $f(a,b)=b$，则 $P(a,f(a,b))=P(a,b)=1$。就是说在给定解释后，用个体域 D 上的每一个元素取代公式 $P(a,f(a,x))$ 中的变元 x 所得命题均为真命题。因此 $(\forall x)P(a,f(a,x))$ 是一个在给定解释之下 D 上总为真的命题。

在给定一个解释下总是真的公式，不一定在所有解释下都是真的。在谓词演算中，有一种在任何可能解释下均为真的所谓普遍有效公式。

定义 2.31 设 A 是谓词公式。

1．A 是**普遍有效**的，当且仅当用任意确定的谓词或命题分别指派 A 中每一个谓词符号和命题变元（零元谓词），用任意确定的函数指派 A 中每一个函数符号，用任意确定的个体指派 A 中的每一个自由个体变元之后，公式 A 总是转化为一个真命题。

2．A 是可满足的，当且仅当用特定谓词、特定命题、特定函数和特定个体指派 A 中每一个自由个体变元之后，它转化为真的命题。

显然，上面例 2.45 中公式 $P(a,f(a,x))$ 不是普遍有效的。因为如果令 $P(a,b)=0$，对这样定义的谓词，$P(a,f(a,x))$ 就不会总是真的。

以下是一些普遍有效的公式（注意，它们各源于表 2.14 中的式（10）和式（11））。

$(\forall x)P(x,y)\vee\neg(\forall x)P(x,y)$

$((\exists x)P(x)\rightarrow(\forall x)Q(x))\rightleftarrows(\neg(\exists x)P(x)\vee(\forall x)Q(x))$

定义 2.32 设 A,B 是两个谓词公式，具有共同的个体域 D。A 与 B 在 D 上是等价的，当且仅当 A,B 中任意相同谓词、函数符号均用同一确定的谓词和函数替代；任意相同的自由个

体变元均用 D 中同一确定的个体代换后，A 和 B 均是真的或者均是假的。

在 D 是全总个体域的情况下，称 A 与 B 是等价的，以符号“$A \Leftrightarrow B$”表示。

显然，$A \Leftrightarrow B$ 即意味着在任何对谓词函数符号和个体变元的代换下，公式 $A \rightleftarrows B$ 是普遍有效的。

定义 2.33 设 A,B 是两个谓词公式，具有共同个体域 D。在 D 上 A 蕴含 B，当且仅当 A,B 中任意相同谓词，函数符号均用同一确定的谓词和函数替代，任意相同的自由个体变元均用 D 中同一确定的个体代换后，若 A 是真的，则 B 也必是真的。

在 D 是全总个体域时，称 A 蕴含 B，以符号“$A \Rightarrow B$”表示。

同样，以下事实是明显的。$A \Rightarrow B$ 即意味着在任何对谓词函数符号和个体变元的代换下，公式 $A \rightarrow B$ 是普遍有效的。

下面是几类基本的等价式和蕴含式。

1．命题演算的推广

在本章的 2.4.2 小节里介绍过对一个命题公式中的同一命题变元均以同一公式置换而得到置换例式的情况。并且，对一个永真式做出的任何置换例式也是永真式。如果用以置换一个永真式中命题变元的是任意的合式的谓词公式的话，显然所得的就是谓词演算中的普遍有效公式。考虑到定义 2.32 和定义 2.33，所以，本章的表 2.14 和表 2.15 中的等价关系和蕴含关系在其中的命题变元看成是任意原子谓词公式的话，它们就是一些谓词演算中的等价式和蕴含式了。例如有

$A(x,y) \rightarrow B(x,y) \Leftrightarrow \neg A(x,y) \vee B(x,y)$

$\neg \neg A(x) \Leftrightarrow A(x)$

$A(x) \wedge (A(x) \rightarrow B(x)) \Rightarrow B(x)$等等。

在给出下面的一些关系式之前，我们先来介绍在论域 D 是有限集时，如何化去公式中量词的方法。

从全称量词的含义可知，$(\forall x)P(x)$表示“对论域 D 中的每一个个体而言，它们都有性质 P”。设 $D=\{a_1,a_2,\cdots,a_n\}$，因此可用合取式来表示上述含有全称量词的公式，即

$$(\forall x)P(x) \Leftrightarrow P(a_1) \wedge P(a_2) \wedge \cdots \wedge P(a_n) \qquad (2.3)$$

而$(\exists x)P(x)$的含义是“论域中有一个个体，它具有性质 P”，所以，以析取式将它们转化为以下命题也是合理的

$$(\exists x)P(x) \Leftrightarrow P(a_1) \vee P(a_2) \vee \cdots \vee P(a_n) \qquad (2.4)$$

2．关于量词和联结词“¬”的等价式

先让我们来看一个例子。

【例 2.46】 设 $A(x)$表示“x 是生物”。则

（1）$(\forall x)A(x)$

表示“所有事物都是生物”。当然它是假的，于是

（2）$\neg(\forall x)A(x)$

表示“并非所有事物都是生物”。这是一个真语句。分析它的含义可知，其表示万物中至少有一个不是生物，即可表示为$(\exists x) \neg A(x)$。它是与以上语句（2）本质上相同的，是真语句。若

不恰当地将语句（1）的否定表示为$(\forall x)\neg A(x)$，就成了“所有的事物都不是生物”，显然这也是一个假语句。

又设 $M(x)$表示“x 是人”。则有

（3）$(\exists x)M(x)$

这个语句表达了“宇宙万物中，有一些是人”，它是真语句。于是

（4）$\neg(\exists x)M(x)$

表示“并非存在一些事物是人”，这是一假语句。分析它的含义可知，它表示所有事物都不是人，即可表示为$(\forall x)\neg M(x)$。它是与以上语句（4）本质上相同的，是假语句。若不恰当地将语句（3）的否定表示为$(\exists x)\neg M(x)$，那么就成了“有一些事物不是人”。它仍是一个真命题，显然这并不是语句（3）的否定。综上所述，我们得到以下两个等价式

$$\neg(\forall x)P(x)\Leftrightarrow(\exists x)\neg P(x) \tag{2.5}$$

$$\neg(\exists x)P(x)\Leftrightarrow(\forall x)\neg P(x) \tag{2.6}$$

在有限个体域 $D=(a_1,a_2,\cdots,a_n)$的情况下，我们可证明公式 2.5（公式 2.6 留做练习）。

$$\begin{aligned}&\neg(\forall x)P(x)\\&\Leftrightarrow\neg(P(a_1)\wedge P(a_2)\wedge\cdots\wedge P(a_n))\\&\Leftrightarrow\neg P(a_1)\vee\neg P(a_2)\vee\cdots\vee\neg P(a_n)\\&\Leftrightarrow(\exists x)\neg P(x)\end{aligned}$$

本节前面曾指出，表示“所有是 P 的对象都是 Q”应当用带全称量词的含有条件联结词的形式：$(\forall x)(P(x)\rightarrow Q(x))$，并说过由此可推知表示“有一个是 P 的对象，它是 Q”必须表示成为“$(\exists x)(P(x)\wedge Q(x))$”。现在通过以下例子来说明。

【例 2.47】 设 $M(x)$：x 是人。$L(x)$：x 是左撇子。于是“所有人都不是左撇子”被表示成

$$(\forall x)(M(x)\rightarrow\neg L(x))$$

它是假语句。其否定“并非所有人都不是左撇子”，意思是“有些人是左撇子”，是一个真语句，用公式表示为

$$\begin{aligned}&\neg(\forall x)(M(x)\rightarrow\neg L(x))\\&\Leftrightarrow\neg(\forall x)(\neg M(x)\vee\neg L(x))\\&\Leftrightarrow\neg(\forall x)\neg(M(x)\wedge L(x))\\&\Leftrightarrow(\exists x)\neg\neg(M(x)\wedge L(x))\\&\Leftrightarrow(\exists x)(M(x)\wedge L(x))\end{aligned}$$

3．量词辖域的扩张与收缩

$$(\forall x)(P(x)\wedge H)\Leftrightarrow(\forall x)P(x)\wedge H \tag{2.7}$$

$$(\forall x)(P(x)\vee H)\Leftrightarrow(\forall x)P(x)\vee H \tag{2.8}$$

$$(\exists x)(P(x)\wedge H)\Leftrightarrow(\exists x)P(x)\wedge H \tag{2.9}$$

$$(\exists x)(P(x)\vee H)\Leftrightarrow(\exists x)P(x)\vee H \tag{2.10}$$

特别要指出的是，H 表示一个不含约束变量 x 的公式。

由这些关系式，还可推出以下几个关系式

$$(\exists x)(P(x)\rightarrow H)\Leftrightarrow(\forall x)P(x)\rightarrow H \tag{2.11}$$

$$(\forall x)(P(x)\rightarrow H)\Leftrightarrow(\exists x)P(x)\rightarrow H \tag{2.12}$$

$$(\exists x)(H\rightarrow P(x))\Leftrightarrow H\rightarrow(\exists x)P(x) \tag{2.13}$$

$$(\forall x)(H\rightarrow P(x))\Leftrightarrow H\rightarrow(\forall x)P(x) \tag{2.14}$$

作为例子，我们证明式（2.12）。

【例 2.48】 证明$(\forall x)(P(x)\rightarrow H)\Leftrightarrow(\exists x)P(x)\rightarrow H$

证明 $(\forall x)(P(x)\rightarrow H)$

$$\Leftrightarrow(\forall x)(\neg P(x)\vee H)$$

$$\Leftrightarrow(\forall x)\neg P(x)\vee H$$

$$\Leftrightarrow\neg(\exists x)P(x)\vee H$$

$$\Leftrightarrow(\exists x)P(x)\rightarrow H$$

4．关于量词对谓词公式的分配

$$(\forall x)(P(x)\wedge Q(x))\Leftrightarrow(\forall x)P(x)\wedge(\forall x)Q(x) \tag{2.15}$$

$$(\exists x)(P(x)\vee Q(x))\Leftrightarrow(\exists x)P(x)\vee(\exists x)Q(x) \tag{2.16}$$

另外还有两个蕴含式

$$(\forall x)P(x)\vee(\forall x)Q(x)\Rightarrow(\forall x)(P(x)\vee Q(x)) \tag{2.17}$$

$$(\exists x)(P(x)\wedge Q(x))\Rightarrow(\exists x)P(x)\wedge(\exists x)Q(x) \tag{2.18}$$

以上公式（2.15）、公式（2.16）不难在有限个体域下证明。至于公式（2.17）、公式（2.18）这里仅通过举例来说明。令 $P(x)$：x 学习好，$Q(x)$：x 身体好，则公式（2.17）以某一学习班为个体域时，表示“所有学生都学习好或者所有学生都身体好蕴含班上每一学生或者学习好或者身体好”。可是相反方面的蕴含是不成立的。例如有甲同学学习好但身体不好，有乙同学却相反，身体好而学习却不好，虽然这不能影响“每一同学或者学习好或者身体好”是真的，但“所有学生都学习好或者所有学生都身体好”却是假的。

这一组关系式中，还有两个蕴含式

$$(\forall x)(P(x)\rightarrow Q(x))\Rightarrow(\forall x)P(x)\rightarrow(\forall x)Q(x) \tag{2.19}$$

$$(\forall x)(P(x)\rightleftarrows Q(x))\Rightarrow(\forall x)P(x)\rightleftarrows(\forall x)Q(x) \tag{2.20}$$

我们来给出式（2.19）的逻辑含义。它的左边肯定了论域的某一个子集的每一个成员“都是 Q”，该子集由论域中所有具有性质“P”的个体 x 组成，即“x 是 P”。而它的右边肯定的是只有论域中的所有个体都是 P，则才有论域中的每一个是 Q。式（2.19）揭示了这样一个逻辑规律：当一个集合（其成员有性质 P）的一个个体有某一性质 Q，则一个由具有该性质 P 的个体组成的集合的全体当然也有性质 Q。例如，$P(x)$：x 到达出发地。$Q(x)$：x 可以出发。显然，如果每一个人（不必是全体）到达出发地他就可以出发，那么当所有人都到达时，所有人可以出发是对的。反之不然。

5．关于多个量词的关系式

先来考察一下含有多个量词的公式的结构。例如$(\forall x)(\exists y)P(x,y)$，量词$\forall x$ 的辖域是$(\exists y)P(x,y)$，而$\exists y$ 的辖域是 $P(x,y)$，所以可以将此公式写成$(\forall x)((\exists y)P(x,y))$。这样一来，公式$(\exists y)(\forall x)P(x,y)$显然就与上述公式有不同的结构。不仅如此，这两个公式的含义也不一样。若在全体整数域上讨论，而 $P(x,y)$表示“x 大于 y”，则以上两个公式可以翻译成这样：

$(\forall x)(\exists y)P(x,y)$表达的是每一个整数均大于某一个整数（对于每一个整数而言，总有一个

比它小的存在)。

$(\exists y)(\forall x)P(x,y)$有一个整数小于所有整数。

我们知道，前一句是一真语句，因为对任何一个整数，当它确定之后都可找到一个比它小的整数存在，因为全体整数没有最小的一个。可是后一语句是假的，原因就是上面说的不存在最小的整数。

$$(\forall x)(\forall y)P(x,y)\Leftrightarrow(\forall y)(\forall x)P(x,y) \tag{2.21}$$

$$(\exists x)(\exists y)P(x,y)\Leftrightarrow(\exists y)(\exists x)P(x,y) \tag{2.22}$$

这是两个等价式，其成立是明显的。还有一些蕴含式

$$(\forall x)(\forall y)P(x,y)\Rightarrow(\exists y)(\forall x)P(x,y) \tag{2.23}$$

$$(\exists y)(\forall x)P(x,y)\Rightarrow(\forall x)(\exists y)P(x,y) \tag{2.24}$$

$$(\forall x)(\exists y)P(x,y)\Rightarrow(\exists y)(\exists x)P(x,y) \tag{2.25}$$

对此，我们不再给予证明，读者不妨自己通过分析每一公式的含义进行推证。

2.12 谓词演算的推理理论

谓词演算的推理是包含谓词公式的推理过程，是命题演算推理理论的推广。命题演算规定的 *P*,*T*,*CP* 规则，也可在谓词演算的推理中使用。不过由于谓词演算中引入了量词和自由变量以及约束变量和论域等，所以它的推理理论要复杂得多。尚需引入四条有关量词的规则以及使用它们时的一些限制。

先从几个蕴含式开始。以下均以记号 $A(x)$表示某一个含有 *x* 是自由出现的公式。例如 $P(x)\wedge(\exists y)Q(y,z)$，$P(x)\rightarrow((\exists y)Q(x,y))$。进一步，若 $A(x)$中的自由变量 *x* 不同时出现在同一公式关于别的约束变量（如 *y*）的辖域中，则可以用 *y* 取代 *x*（当然 *y* 也不能与公式中其他自由变量同名），并且说公式 $A(x)$对 *y* 是自由的。也即用 *y* 取代 *x* 以后，不会改变原公式的结构。上面列举到的那两个公式，第一个对 *y* 是自由的，另一个对 *y* 不是自由的。下面的讨论中，凡是出现以 *y* 代换 $A(x)$中的 *x* 而得到 $A(y)$的情况时，都假定 $A(x)$对 *y* 自由的。

$$(\forall x)A(x)\Rightarrow A(y) \tag{2.26}$$

为证式（2.26），假设$(\forall x)A(x)$是真的。显然 $A(y)$在任何解释下为真。

设 *H* 是一不含变量 *x* 的自由出现的公式，于是

$$H\rightarrow A(x)\Rightarrow H\rightarrow(\forall x)A(x) \tag{2.27}$$

事实上，若 $H\rightarrow A(x)$在任何解释下都真，特别地当 *H* 是真，则对每一个对象 *x*，$A(x)$都真，由于 *x* 不在 *H* 中自由出现，那么改变 *x* 为约束出现，将不改变 *H* 的真值，所以 $H\rightarrow(\forall x)A(x)$必定是真的。

作为式（2.27）的特例，有

$$(P\vee\neg P)\rightarrow A(x)\Rightarrow(P\vee\neg P)\rightarrow(\forall x)A(x)$$

考虑到本章习题 2.14（b），于是可以得到

$$A(x)\Rightarrow(\forall x)A(x) \tag{2.28}$$

在和式（2.26）及式（2.28）类似的假设下，还可得到另外两个蕴含式

$$(\exists x)A(x)\Rightarrow A(y) \tag{2.29}$$

$$A(y)\Rightarrow(\exists x)A(x) \tag{2.30}$$

式（2.26）称为**全称特指规则** *US*，式（2.28）称为**全称推广规则** *UG*，式（2.29）称为存

在特指规则 *ES*，式（2.30）称为**存在推广规则** *EG*。不过在推理中使用它们的时候，必须注意某些重要的限制。

规则 *US*：从$(\forall x)A(x)$可以推出 $A(y)$。

规则 *ES*：从$(\exists x)A(x)$可以推出 $A(y)$。但必须保证 y 在任意前提中不是自由出现的和前面任一步推导中 y 也不是自由出现的。我们可以容易地用每次使用 *ES* 时，引入一个新变量的方法满足这一要求。

规则 *UG*：从 $A(x)$可以推出$(\forall y)A(y)$。但是必须保证 x 在任意一个前提中都不是自由的，并且如果 $A(x)$是一个由 *ES* 引入的公式，则对此公式中任意一个由 *ES* 引入的，形式上自由出现的变元，均不可引用此规则。

规则 *EG*：从 $A(x)$可以推出$(\exists y)A(y)$。

除要求 $A(x)$对 y 是自由的之外，规则 *US* 和 *EG* 不要求任何限制均可以引用。而 *UG* 和 *ES* 的种种限制，主要是推理的前提和中间每一步骤引入的公式一般都不是普遍有效（或永真）的，只是保证当前提均假设为有效的话，蕴含以后每一步上引入的公式也有效。即任何一步上引入的公式，若不是一个假定有效的前提，则它一定被它前面一些步骤上引入的公式所蕴含。但这种蕴含的成立，往往依赖于公式中变元的可取值的域。例如 *ES* 规则，从$(\exists x)A(x)$引入公式$A(y)$。如不限制在各前提和先于它导出的公式中 y 必须是约束出现的，则$(\exists x)A(x) \Rightarrow A(y)$可能不成立。因为$(\exists x)A(x)$为真，并不蕴含对每一个 y 都有 $A(y)$为真。$A(y)$中，*ES* 规则里的 y 只是形式上为自由出现而已，实际上它可以在其中取值的域只是使 $A(y)$为真的那些个体的集合。

限于本教材的性质，不再深入讨论这些问题。在现阶段，我们给大家一个谓词逻辑推理的限制，即前提中不出现任何自由变元[*]。也即，前提中不出现命题函数（注意，确定的个体，如*s*：苏格拉底，不属于自由变元。参看以下的例 2.49）。下面举一个例子说明在论证中违背了规则要遵循的限制后，是如何引出错误的结论的。

设 $D(u,v)$：v 可以整除 u，个体域是正整数。则$(\exists u)D(u,5)$是真的。因为 $D(5,5)$，$D(20,5)$等是真的。考虑以下证明：

（1）$(\exists u)D(u,5)$	*P*；
（2）$D(x,5)$	*ES*；（1）（x 被 *ES* 引入）
（3）$(\forall y)D(y,5)$	*UG*；（2）

显然结论$(\forall y)D(y,5)$是假的，是错误的。因为在（3）步上，违反了 *UG* 的第 2 个限制。在（2）步上，用 *ES* 引入了变量 x，形式上它在 $D(x,5)$中是自由出现的，而第（3）步上又对公式 $D(x,5)$中变量 x 不恰当地引用了 *UG*。

最后给出几个例题，熟悉一下谓词演算的推理。

【例 2.49】 证明本章的第 9 节一开始提出的“苏格拉底三段论”的正确性。

证明 设 *s*：苏格拉底，$M(x)$：x 是人。

$D(x)$：x 要死的。

前提是$(\forall x)(M(x) \rightarrow D(x))$，$M(s)$（上面已经提到过，$s$ 不是个体变元，所以 $M(s)$不是命题函数，而是一个确定的命题！）

[*] 这个限制并不是必须的。只要充分考虑了不会违背使用规则 *UG* 和 *ES* 的限制就行。参阅本章练习 2.40（C）。

结论是 $D(s)$

（1）$(\forall x)(M(x)\rightarrow D(x))$　　P；

（2）$M(s)\rightarrow D(s)$　　US；（1）

（3）$M(s)$　　P；

（4）$D(s)$　　T；（2），（3）

【例 2.50】 试证有$(\exists x)(P(x)\wedge Q(x))\Rightarrow(\exists x)P(x)\wedge(\exists x)Q(x)$

证明 （1）$(\exists x)(P(x)\wedge Q(x))$　　P；

（2）$P(y)\wedge Q(y)$　　ES；（1）；（y 被 ES 引入）

（3）$P(y)$　　T；（2）

（4）$Q(y)$　　T；（2）

（5）$(\exists x)P(x)$　　EG；（3）

（6）$(\exists x)Q(x)$　　EG；（4）

（7）$(\exists x)P(x)\wedge(\exists x)Q(x)$　　T；（5），（6）

又知，证明的逆问题是不成立的。来看一个关于此逆问题的错误证明。

（1）$(\exists x)P(x)\wedge(\exists x)Q(x)$　　P；

（2）$(\exists x)P(x)$　　T；（1）

（3）$(\exists x)Q(x)$　　T；（1）

（4）$P(y)$　　ES；（2）；（y 被 ES 引入）

（5）$Q(y)$　　ES；（3）

（6）$P(y)\wedge Q(y)$　　T；（4），（5）

（7）$(\exists x)(P(x)\wedge Q(x))$　　EG；（6）

错误出在第（5）步上。它引入的 y 在第（4）步上已经自由出现过。所以只能将第（5）步改为 $Q(z)$。于是论证就无以为继了。

【例 2.51】 试证明由前提

（1）$(\forall x)(P(x)\rightarrow(Q(x)\wedge R(x)))$；

（2）$(\exists x)(P(x)\wedge W(x))$；

可有效推出结论$(\exists x)(R(x)\wedge W(x))$

证明 （1）$(\forall x)(P(x)\rightarrow(Q(x)\wedge R(x)))$　　P；

（2）$(\exists x)(P(x)\wedge W(x))$　　P；

（3）$P(y)\wedge W(y)$　　ES；（2）；（y 被引入）

（4）$P(y)\rightarrow(Q(y)\wedge R(y))$　　US；（1）

（5）$P(y)$　　T；（3）；

（6）$W(y)$　　T；（3）

（7）$Q(y)\wedge R(y)$　　T；（4），（5）

（8）$R(y)$　　T；（7）

（9）$R(y)\wedge W(y)$　　T；（6），（8）

（10）$(\exists x)(R(x)\wedge W(x))$　　EG；（9）

不要希望从第（9）步的 $R(y)\wedge W(y)$推出$(\forall x)(R(x)\wedge W(x))$。因为在第（3）步上，$y$ 被 ES 引入。另外，第（3）步和第（4）步不能交换。

习　题

2.1．指出以下语句中，哪些是命题，哪些不是。

（a）离散数学是计算机科学系的一门必修课。

（b）你有空吗?

（c）请勿吸烟。

（d）不存在最大的质数。

（e）9+5＞18。

（f）如果天下雨，就不去公园。

2.2　举例说明原子命题和复合命题。

2.3　用语句

S：张军是健壮的。

C：张军是聪明的。

把下列语句写成符号形式：

（a）张军是聪明的也是健壮的。

（b）张军是健壮的或者是不聪明的。

（c）张军既不是健壮的也不是聪明的。

（d）张军并不是又健壮又聪明。

2.4　用汉语写出语句，使之对应以下各形式语言。

（a）$(P\vee Q)\rightarrow R$;

（b）$\neg P\wedge\neg Q$;

（c）$(P\rightarrow Q)\wedge(Q\rightarrow P)$。

2.5　指出下列命题中的原子命题。

（a）天气又热又不下雨。

（b）小王小李都进城去了。

（c）如果你不去，那么我也不去。

2.6　下面给出的式子里，哪些是合式的，并指出哪些合式公式是永真式或永假式。

（a）$(P\rightarrow(P\vee Q))$;

（b）$((P\rightarrow\neg P)\rightarrow\neg P))$;

（c）$((\neg Q\wedge P)\wedge Q)$;

（d）$(P\wedge Q)\rightleftarrows P)$;

（e）$(\neg(P\rightleftarrows Q)\rightleftarrows(\neg P\rightleftarrows Q))$。

2.7　将下列语句符号化。

（a）或者你没给我写信，或者信丢了。

（b）如果张和李都不参加这次活动，那王就去参加。

（c）我们不能既划船又去跳舞。

（d）如果你在，他是否演唱就取决于你是否伴奏了。

（e）除非天上下钉子，否则我去 B 城。

2.8　求下列命题公式的真值表。

（a）$P\rightarrow(Q\vee R)$；

（b）$(P\vee Q)\rightarrow(P\rightarrow Q)$；

（c）$(P\rightarrow(Q\rightarrow R))\rightarrow((P\rightarrow Q)\rightarrow(P\rightarrow R))$。

2.9　试证明以下各式为永真式。

（a）$(P\rightarrow Q)\rightarrow(\neg P\vee Q)$；

（b）$(P\rightarrow Q)\rightleftarrows(\neg P\vee Q)$；

（c）$((\neg P\wedge\neg Q\wedge R)\vee(Q\wedge R)\vee(P\wedge R))\rightarrow R$。

2.10　在下列各式中，求以$(P\rightarrow Q)$置换 P，以$(Q\vee R)$置换 Q 所得的置换例式。

（a）$(\neg P\vee W)\rightarrow(Q\vee R)$；

（b）$P\rightarrow(Q\rightarrow R)$。

2.11　试以真值表证明以下等价关系：

（a）合取式的结合律；

（b）合取对析取的分配律；

（c）摩根律。

2.12　不构造真值表，证明以下等价关系：

（a）$A\rightarrow(B\rightarrow A)\Leftrightarrow\neg A\rightarrow(A\rightarrow\neg B)$；

（b）$\neg(A\rightleftarrows B)\Leftrightarrow(A\vee B)\wedge\neg(A\wedge B)$；

（c）$\neg(A\rightleftarrows B)\Leftrightarrow(A\wedge\neg B)\vee(\neg A\wedge B)$；

（d）$(A\rightarrow P)\wedge(B\rightarrow P)\Leftrightarrow(A\vee B)\rightarrow P$。

2.13　构造真值表证明以下蕴含关系：

（a）$(P\wedge Q)\Rightarrow P\rightarrow Q$；

（b）$(P\rightarrow(Q\rightarrow R))\Rightarrow(P\rightarrow Q)\rightarrow(P\rightarrow R)$。

2.14．不构造真值表证明以下蕴含关系：

（a）$P\rightarrow Q\Rightarrow P\rightarrow(P\rightarrow Q)$；

（b）$((P\vee\neg P)\rightarrow Q)\rightarrow((P\vee\neg P)\rightarrow R)\Rightarrow Q\rightarrow R$；

（c）$(Q\rightarrow(P\wedge\neg P))\rightarrow(R\rightarrow(P\wedge\neg P))\Rightarrow R\rightarrow Q$。

2.15　化简以下各式：

（a）$((A\rightarrow B)\rightleftarrows(\neg B\rightarrow\neg A))\wedge C$；

（b）$(A\wedge B\wedge C)\vee(\neg A\wedge B\wedge C)$；

（c）$(\neg A\wedge B\wedge C)\vee(A\wedge\neg B\wedge\mathrm{C})\vee(A\wedge B\wedge\neg C)\vee(A\wedge B\wedge C)$。

2.16　若 $A\Leftrightarrow B$。是否有 $A\vee C\Leftrightarrow B\vee C$？为什么？反之如何？是否有 $A\wedge C\Leftrightarrow B\wedge C$？反之如何？

2.17　证明以下公式是永真的：

（a）$(P\wedge(P\rightarrow Q))\rightarrow Q$；

（b）$\neg P\rightarrow(P\rightarrow Q)$；

（c）$((P\rightarrow Q)\wedge(Q\rightarrow R))\rightarrow(P\rightarrow R)$。

2.18　求以下公式的析取范式（析取范式是初等积的析取式，它不必是主析取范式）：

（a）$P\wedge(P\rightarrow Q)$；

（b）$P\rightarrow((Q\wedge R)\rightarrow S)$；

（c）$\neg(P\wedge Q)\wedge(P\vee Q)$。

2.19 求下列公式的合取范式（合取范式是初等和的合取式，它不必是主合取范式）。

（a）$P\vee(\neg P\wedge Q\wedge R)$；

（b）$(\neg P\wedge Q)\vee(P\wedge\neg Q)$；

（c）$P\rightarrow((Q\wedge R)\rightarrow S)$。

2.20 求以下公式的主析取范式和主合取范式。

（a）$(\neg P\rightleftarrows Q)\rightarrow(P\vee Q)$；

（b）$(P\rightleftarrows\neg Q)\rightarrow(P\wedge Q)$；

（c）$\neg P\vee Q$；

（d）$(P\vee Q)\rightarrow(Q\wedge R)$。

2.21 先求出以下各式的主析取范式，然后根据其主析取范式直接写出主合取范式。

（a）$\neg(P\rightarrow Q)$；

（b）$(P\rightarrow(Q\wedge R))\wedge(P\rightarrow(\neg Q\wedge\neg R))$。

2.22 用推理规则证明以下各式。

（a）$\neg(P\wedge\neg Q),\neg Q\vee\mathrm{R},\neg R\Rightarrow\neg P$；

（b）$Q,\neg P\rightarrow R,P\rightarrow S,\neg S\Rightarrow Q\wedge R$；

（c）$P\wedge Q,Q\rightarrow\neg R,R\vee S\Rightarrow S$；

（d）$P\rightarrow Q,(\neg Q\vee R)\wedge\neg R,\neg(\neg P\wedge S)\Rightarrow\neg S$。

2.23 只用规则 P 和 T 论证。

（a）$\neg A\vee B,C\rightarrow\neg B\Rightarrow A\rightarrow\neg C$；

（b）$\neg A\vee B,\neg B\vee C,C\rightarrow D\Rightarrow A\rightarrow D$；

（c）$P\rightarrow Q\Rightarrow P\rightarrow(P\wedge Q)$；

（d）$(P\vee Q)\rightarrow R\Rightarrow(P\wedge Q)\rightarrow R$；

（e）$A\rightarrow(B\rightarrow C),(C\wedge D)\rightarrow E,\neg H\rightarrow(D\wedge\neg E)\Rightarrow A\rightarrow(B\rightarrow H)$。

提示：考虑等价式 $P\rightarrow(Q\rightarrow R)\Leftrightarrow(Q\wedge P)\rightarrow R$。

2.24 用规则 *CP* 证明 2.23 题各式。

2.25 推理证明以下各式，必要时可用反证法。

（a）$P\Rightarrow(\neg P\rightarrow Q)$；

（b）$(R\rightarrow\neg Q), R\vee S, S\rightarrow\neg Q, P\rightarrow Q\Rightarrow\neg P$；

（c）$P\rightarrow\neg Q, P\vee R, \neg R, \neg R\rightleftarrows Q\Rightarrow\neg S$；

提示：前提不相容。

（d）$\neg(P\rightarrow Q)\rightarrow\neg(R\vee S), (Q\rightarrow P)\vee\neg R, R\Rightarrow P\rightleftarrows Q$；

（e）$P\rightarrow Q\Rightarrow(P\wedge R)\rightarrow Q$；

（f）$P\rightarrow Q\Rightarrow P\rightarrow(Q\vee R)$；

（g）$P\rightarrow Q, R\rightarrow S\Rightarrow(P\wedge R)\rightarrow(Q\wedge S)$；

（h）$P\rightarrow Q, R\rightarrow S\Rightarrow(P\vee R)\rightarrow(Q\vee S)$。

2.26 证明以下论证是有效的。

我母亲生日时，我献一束花给她。

今天或者是我母亲的生日或者我上课迟到了。

我没有给我母亲献花。

所以，

今天我上课迟到了。

2.27　用谓词表达式符号化以下语句。

（a）小张不是工人。

（b）他是田径或足球运动员。

（c）若 m 是奇数，则 $m+1$ 不是奇数。

（d）张是三好学生而李不是。

2.28　将以下语句表达成谓词合式公式。

（a）每一个有理数都是分数。

（b）有些人不爱吃菠菜。

（c）并非所有连续函数都是可微分的。

（d）如果全世界的所有人都爱和平，世界将不再有战争。

（e）宇宙间任何事物都是变化的。

（f）如果万物都是变化的，那么小王也要变。

2.29　设 $R(x)$：x 是无理数，那么$(\exists x)R(x)$在（a）全总个体域；（b）有理数域；（c）实数域上各表示真命题还是假命题抑或是一种不恰当的表述？

2.30　令 $P(x)$：x 是质数；$E(x)$：x 是偶数；

$O(x)$：x 是奇数；$D(x,y)$：x 整除 y。

把以下各式翻译成汉语的语句（个体域是整数集）。

（a）$(\forall x)(D(2,x)\rightarrow E(x))$；

（b）$(\exists x)(E(x)\wedge D(x,6))$；

（c）$(\forall x)(\neg E(x)\rightarrow\neg D(2,x))$；

（d）$(\forall)(E(x)\rightarrow(\exists y)(E(y)\wedge D(y,x)))$；

（e）$(\forall x)(P(x)\rightarrow(\forall y)(E(y)\rightarrow\neg D(x,y)))$。

2.31　将以下语句符号化，使之成为合式的谓词公式。

（a）两个数之积为零，则两数中必有一个是零。

（b）有一个人，比所有人都不矮。

（c）每一个人都比某一个人高。

（d）函数极限的定义：$\lim\limits_{x\to a} f(x)=b$。

2.32　下面哪些是语句？

（a）$(\forall x)(P(x)\wedge Q(x))\vee R$（$R$ 是一个命题）；

（b）$(\forall x)(P(x)\wedge Q(x))\vee(\exists x)S(x,y)$；

（c）$(\forall x)(P(x)\wedge Q(x))\vee(\exists x)S(x)$。

2.33　指出自由变量和约束变量以及量词的辖域。

（a）$(\forall x)(P(x)\rightarrow Q(x))\vee R(x)$；

（b）$(\forall x)(P(x)\rightarrow(\forall x)(Q(x)\rightarrow R(x)))\vee S(x)$；

（c）$(\forall x)(\exists y)(P(x,y)\rightarrow R(z,x))$。

2.34　设论域是$\{a,b,c\}$，消去以下公式的量词。

（a）$(\forall x)(P(x)\rightarrow Q(x))$；

（b）$(\exists x)P(x)\wedge(\exists y)Q(y)$；

（c）$(\forall x)\neg P(x)\vee(\forall x)P(x)$。

2.35　试求以下公式在给出的解释 I 之下的真值。

（a）$(\forall x)(P(x)\vee Q(x))$

I：$\frac{P(1)}{1},\frac{P(2)}{0},\frac{Q(1)}{0},\frac{Q(2)}{1}$；论域 $D=\{1,2\}$

（b）$(\exists x)(P(f(x))\wedge Q(x,f(a)))$

I：$D=\{2,3\}$

$$\frac{a}{2},\frac{f(2)}{3},\frac{f(3)}{2},\frac{P(2)}{0},\frac{P(3)}{1}$$

$$\frac{Q(2,2)}{1},\frac{Q(2,3)}{1},\frac{Q(3,2)}{0},\frac{Q(3,3)}{1}$$

（c）$(\forall x)(P(x)\rightarrow Q(x,a))$

在与（b）相同的解释下。

2.36　将下列公式中的约束变量 x 换名。

（a）$(\forall x)(P(x,y)\vee S(x))\rightarrow R(y)$；

（b）$(\exists x)P(x,y)\vee(S(y)\wedge(\forall x)R(x,u))$；

（c）$(\forall x)(\forall y)(P(x,y)\rightarrow Q(x,y))\vee R(x,y)$。

2.37　将下列公式中的自由变量 x 换成一个新变量。

（a）$(\exists x)(P(x,y)\vee Q(x,z))\vee R(x)$；

（b）$P(x,y)\wedge((\forall x)Q(x)\rightarrow R(x))$；

（c）$((\exists u)(P(x,u)\wedge R(x))\rightarrow(\forall x)P(x,y))\vee S(x,z)$。

2.38．下面这些公式中，哪些 $A(x)$ 对变量 y 是自由的？

（a）$A(x)=(\exists y)(P(u,y)\wedge Q(y))\vee S(x,z)$；

（b）$A(x)=((\forall x)P(x,y)\rightarrow((\exists y)Q(x,y)\wedge S(x)))\rightarrow R(s,x)$；

（c）$A(x)=(\forall y)P(y)\rightarrow(((\exists x)Q(x)\wedge R(x))\wedge A(x))$。

2.39　证明下列各式。

（a）$(\exists x)(A(x)\rightarrow B(x))\Leftrightarrow(\forall x)A(x)\rightarrow(\exists x)B(x)$；

（b）$(\forall x)A(x)\vee(\forall x)B(x)\Rightarrow(\forall x)(A(x)\vee B(x))$；

（c）$(\forall x)(\forall y)(P(x)\rightarrow Q(y))\Leftrightarrow(\exists x)P(x)\rightarrow(\forall y)Q(y)$。

2.40　利用谓词演算的推理规则证明下列各式。

（a）$(\forall x)(C(x)\rightarrow(W(x)\wedge R(x))),(\exists x)(C(x)\wedge Q(x))\Rightarrow(\exists x)(Q(x)\wedge R(x))$；

（b）$(\forall x)(H(x)\rightarrow M(x)),(\exists x)H(x)\Rightarrow(\exists x)M(x)$；

（c）$P(x)$*，$(\forall x)Q(x)\Rightarrow(\exists x)(P(x)\wedge Q(x))$；

（d）$(\forall x)(P(x)\vee Q(x))$，$(\forall x)(Q(x)\rightarrow\neg R(x))$，$(\forall x)R(x)\Rightarrow(\forall x)P(x)$。

2.41　用 *CP* 规则证明以下各式。

（a）$(\forall x)(P(x)\rightarrow Q(x))\Rightarrow(\forall x)P(x)\rightarrow(\forall x)Q(x)$；

（b）$(\forall x)(P(x)\vee Q(x))\Rightarrow(\forall x)P(x)\vee(\exists x)Q(x)$。

2.42．指出以下推导为什么是错误的。

（a）（1）$(\forall x)P(x)\rightarrow Q(x)$；

---

* 回忆本章 2.12 节内关于 *UG* 规则的一段说明。

（2）$P(x)\rightarrow Q(x)$；

（b）（1）$(\forall x)(P(x)\vee Q(x))$；

（2）$P(a)\vee Q(b)$；

（c）（1）$(\forall x)(P(x)\vee(\exists x)(Q(x)\wedge R(x)))$；

（2）$P(a)\vee(\exists x)(Q(x)\wedge R(a))$。

2.43　试证明：

任何喜欢步行的人都不喜欢乘机动车。

任何人或者喜欢乘机动车或者喜欢骑自行车。

有的人不喜欢骑自行车。

所以，

有些人不喜欢步行。

2.44　指出以下推证错误之处，并改正之。

（1）$(\forall x)(P(x)\vee Q(x))$　　P；

（2）$P(y)\vee Q(y)$　　US；（1）

（3）$(\exists x)\neg P(x)$　　P；

（4）$\neg P(y)$　　ES；（3）

（5）$Q(y)$　　T；（2），（4）

（6）$(\exists x)Q(x)$　　EG；（5）

第 3 章　集合和关系

集合是数学的基本概念之一。本章将简要地用符号逻辑来表达集合概念。因为几乎可以说，没有任何别的方式比用符号化的形式语言来表述集合问题更为合适了。

关系是本章的重点，它是关系数据库的理论基础。函数则更是经常普遍会遇到的概念。而关系和函数却又都是以集合理论作为基础的。所以在集合之后，本章将讨论关系和函数。

3.1　集合和集合的运算

集合是一类事物（或对象）的聚集。以上提到的事物可以是具体的或者抽象的。

3.1.1　集合的基本概念

一般情形下，大写字母 $A,B,\cdots,P,Q,\cdots$，表示集合，小写字母 $a,b,\cdots,x,y,\cdots$，表示组成集合的某一确定对象或元素（准确地说，是对象和元素的名字）。符号 $a\in A$ 的含义是元素 a 是组成集合 A 的一员，$a\notin A$ 则表示 a 不是 A 的一员。

表示一个集合有多种方法。视需要，通常有以下两种方法。

1．列举法　将属于一集合的全体元素罗列成一个序列，并用大括号将它括起来。

一般列举法仅适用于集合所含元素为有限个或无限可列的（如全体自然数 N ）的情形。

2．描述法　给出一个集合的元素的充要条件或者称之为**属性**，用此条件抽象地描述一个集合。这在一般关于集合理论的论述中特别有用。

设 $P(x)$ 表示 x 有属性 P 。那么

$$A=\{x\mid P(x)\}$$

表示的就是一切有性质 P 的元素组成的集合。于是，空集 $\varnothing$ 可表示成

$$\varnothing=\{x\mid\neg P(x)\wedge P(x)\}$$

全总个体域 $\mathbf{E}$ 也称完全集或全集，可表示成

$$\mathbf{E}=\{x\mid\neg P(x)\vee P(x)\}$$

以上 $P(x)$ 可以是任意一个确定的谓词公式。

定义 3.1　设 A,B 是两个集合。A 包含于 B（或 B 包含 A），即，如果 $x\in A$，则有 $x\in B$。

$$(\forall x)(x\in A\rightarrow x\in B)\ ^{*}\qquad(3.1)$$

这时也称 A 是 B 的子集。记为 $A\subseteq B$，或 $B\supseteq A$。

定义 3.2　两集合 A,B 相等，记为 $A=B$。当且仅当 $A\subseteq B$，且 $B\subseteq A$。即

$$A=B\Leftrightarrow(\forall x)(x\in A\rightleftarrows x\in B)\qquad(3.2)$$

集合满足以下定律。

1．自反律　$A\subseteq A$

$$((\forall x)(x\in A\rightarrow x\in A)\Leftrightarrow \mathrm{T}$$

---

* 逻辑联结词“→”等只能连接两个命题，所以省略了命题 $x\in A,x\in B$ 各自外层的括号不致误解。

2．反对称律　$A\subseteq B, B\subseteq A\Rightarrow A=B$

$$(\forall x)(x\in A\rightarrow x\in B),(\forall x)(x\in B\rightarrow x\in A)\Rightarrow A=B$$

3．传递律　$A\subseteq B, B\subseteq C\Rightarrow A\subseteq C$

$$(\forall x)(x\in A\rightarrow x\in B),(\forall x)(x\in B\rightarrow x\in C)\Rightarrow (\forall x)(x\in A\rightarrow x\in C)$$

定义 3.3　A 是 B 的真子集，记做 $A\subset B$，当且仅当

$$A\subset B\Leftrightarrow (A\subseteq B)\wedge (A\neq B) \tag{3.3}$$

依据以上的一些定义，可以推出以下集合的初等性质：

1．对任意确定集合 A，有 $\varnothing\subseteq A, A\subseteq \mathbf{E}, \varnothing\subseteq \mathbf{E}$。

2．$\varnothing\subseteq\varnothing$。

定义 3.4　设 A 是一个集合，由 A 的所有子集为元素组成的集合，叫做 A 的**幂集**，记为 $\rho(A)$，即

$$\rho(A)=\{X\mid X\subseteq A\} \tag{3.4}$$

在 A 的一切子集中，A 本身和 $\varnothing$ 这两个子集又叫平凡子集。

设 A 含有 n 个元素，则容易明白幂集 $\rho(A)$ 含有 2^n 个子集。类似于第 2 章 2.6 节所述小项的编码，也可对集合 A 的每一子集施行编码。

例如，$A=\{a,b\}$，那么它有四个子集：

$$S_0=S_{00}=\{\},\quad S_1=S_{01}=\{b\}$$
$$S_2=S_{10}=\{a\},\quad S_3=S_{11}=\{a,b\}$$

【例 3.1】　给出 $A=\{a\}$ 的幂集 $\rho(A)$。

解　A 的全部子集共两个，就是 $\varnothing$ 和 A

所以　$$\rho(A)=\{\varnothing,\{a\}\}$$

【例 3.2】　在上例中求 $\rho(\rho(A))$。

解　$\rho(\rho(A))=\rho(\{\varnothing,\{a\}\})$

而 $\{\varnothing,\{a\}\}$ 一共有四个子集，它们是

$$\varnothing,\{\varnothing\},\{\{a\}\},\{\varnothing,\{a\}\}$$

所以　$$\rho(\rho(A))=\{\varnothing,\{\varnothing\},\{\{a\}\},\{\varnothing,\{a\}\}\}$$

3.1.2　集合的运算

按照某一确定的规律，从一个或多个已知集合构造出一个新集合的过程叫集合的运算。实际上，上面 3.1.1 节中的幂集就是一种集合的一元运算。

定义 3.5　A,B 是两集合。A,B 的交集 $A\cap B$ 就是

$$A\cap B=\{x\mid x\in A\wedge x\in B\} \tag{3.5}$$

由交集的定义，可直接推出以下交集的初等性质。

1．$A\cap B=B\cap A$ (3.6)

2．$A\cap A=A$ (3.7)

3．$A\cap\varnothing=\varnothing$ (3.8)

4．$A\cap\mathbf{E}=A$ (3.9)

5．$A\cap B\subseteq A, A\cap B\subseteq B$ (3.10)

6．若 $A\subseteq B$，则有 $A\cap B=A$ (3.11)

先来证明 $A\cap B\subseteq A$，即要证（现在我们只有交集、子集的定义可作为前提）

$$(\forall x)(x\in A\cap B\rightarrow x\in A)$$

实际上，任意给定 $x\in A\cap B$，由交集定义推知 $x\in A\wedge x\in B$。因此，$x\in A$。这样就完成了证明。

现在，为证明上面性质 6，由 3.1.1 节中的集合反对称律可知：只要在前提 $A\subseteq B$ 下推出 $A\subseteq A\cap B$ 即可（因为已证明 $A\cap B\subseteq A$）。

设任意一个 $x\in A$，由前提 $A\subseteq B$ 推知 $x\in B$。因此有 $x\in A\wedge x\in B$。最后按交集定义得 $x\in A\cap B$。证得了 $A\subseteq A\cap B$。

当然，以上的证明均可以通过谓词逻辑演算严格规范的形式给出。为节省篇幅，以后涉及类似的证明，均以这种简约的格式给出。作为一次练习，读者不妨将这里的两个证明，用规范的谓词逻辑推理给出。

交运算还满足结合律。

7. $(A\cap B)\cap C=A\cap(B\cap C)$ （3.12）

此结合律可以用归纳法推广到任意有限个集合的情况。于是

$$\bigcap_{i=1}^{n}A_i=A_1\cap A_2\cap\cdots\cap A_n$$

表示唯一确定的集合。

定义 3.6 A,B 是两个集合。若 $A\cap B=\varnothing$，则称 A 和 B 是**不相交**的。

定义 3.7 A,B 是两个集合。A,B 的并集 $A\cup B$ 就是

$$A\cup B=\{x\mid x\in A\vee x\in B\} \quad (3.13)$$

集合的并运算有以下初等性质。

1. $A\cup B=B\cup A$ （3.14）
2. $A\cup A=A$ （3.15）
3. $A\cup\mathbf{E}=\mathbf{E}$ （3.16）
4. $A\cup\varnothing=A$ （3.17）
5. $A\subseteq A\cup B, B\subseteq A\cup B$ （3.18）
6. 若 $A\subseteq B$，则 $A\cup B=B$ （3.19）
7. $(A\cup B)\cup C=A\cup(B\cup C)$ （3.20）

类似地，记

$$\bigcup_{i=1}^{n}A_i=A_1\cup A_2\cup\cdots\cup A_n$$

【例 3.3】 设 $A=\{3,2,\{1\}\}$，$B=\{1,5\}$，$C=\{4,5,6\}$，求出 $A\cap B, A\cup B, A\cap B\cap C$ 和 $A\cup B\cup C$。

解 由交与并的定义可知

$$A\cap B=\varnothing,\ A\cup B=\{1,2,3,\{1\},5\}$$

$$A\cap B\cap C=\varnothing,\ A\cup B\cup C=\{1,2,3,\{1\},4,5,6\}$$

图 3.1 给出两集合交、并和包含关系的**文氏图**。

定义 3.8 A,B 是两个集合。A 和 B 的差集 $A-B$ 就是

$$A-B=\{x\mid x\in A\wedge x\notin B\}$$

$A-B$ 也称为 B 关于 A 的**相对补集**。

定义 3.9 设 $\mathbf{E}$ 是完全集，A 是任一集合。$\mathbf{E}-A$ 是 A 的**绝对补集**（也简称为**补集**），记为 $\sim A$。就是

$$\sim A=\{x\mid x\in \mathbf{E}\wedge x\notin A\}$$

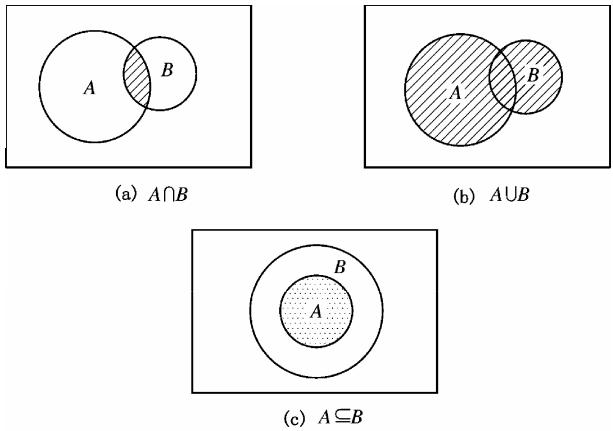


图 3.1　交、并和包含关系的文氏图

集合的补运算有以下初等性质。

1．$\sim(\sim A)=A$　　（3.21）

2．$\sim\varnothing=\mathbf{E}$　　（3.22）

3．$\sim\mathbf{E}=\varnothing$　　（3.23）

4．$A\cup\sim A=\mathbf{E}$　　（3.24）

5．$A\cap\sim A=\varnothing$　　（3.25）

证明是简单的。如

$$A\cup\sim A=\{x\mid x\in A\vee x\notin A\}=\mathbf{E}$$

【例 3.4】　设 $A=\{a,b,c\},B=\{b,e,f\},C=\{d,e\}$。求 $A-B,B-A,(A-C)-B,A-(C-B)$。

解

$$A-B=\{a,c\}\qquad B-A=\{e,f\}$$

$\because$　$$A-C=\{a,b,c\}\qquad C-B=\{d\}$$

$\therefore$　$$(A-C)-B=\{a,c\}\qquad A-(C-B)=\{a,b,c\}$$

以上第一行两式证明了差运算不满足交换律。而最后一行的两个式子证明了差运算不满足结合律。

【例 3.5】　试证明

（a）$A-B=A\cap\sim B$

（b）$A\subseteq B\Leftrightarrow\sim B\subseteq\sim A$

证明　（a）任取一个 x

$$\begin{aligned}x\in(A-B)&\Leftrightarrow x\in\{x\mid x\in A\wedge x\notin B\}\\&\Leftrightarrow x\in\{x\mid x\in A\wedge x\in\sim B\}\\&\Leftrightarrow x\in A\cap\sim B\end{aligned}$$

（b）
$$\begin{aligned}A\subseteq B&\Leftrightarrow(\forall x)(x\in A\rightarrow x\in B)\\&\Leftrightarrow(\forall x)(x\notin B\rightarrow x\notin A)\\&\Leftrightarrow(\forall x)(x\in\sim B\rightarrow x\in\sim A)\end{aligned}$$

$$\Leftrightarrow \sim B \subseteq \sim A$$

【例 3.6】 试证明对任意两个集合 A 和 B，下列等式成立。

$$A-(A\cap B)=A-B \tag{3.26}$$

证明 任取一个 $x\in A-(A\cap B)$，有

$$\begin{aligned}
x\in A-(A\cap B) &\Leftrightarrow x\in\{x\mid x\in A\wedge x\notin(A\cap B)\}\\
&\Leftrightarrow x\in\{x\mid x\in A\wedge\neg\ (x\in A\wedge x\in B)\}\\
&\Leftrightarrow x\in\{x\mid x\in A\wedge(\neg\ (x\in A)\vee\neg\ (x\in B))\}\\
&\Leftrightarrow x\in\{x\mid x\in A\wedge(x\notin A\vee x\notin B)\}\\
&\Leftrightarrow x\in\{x\mid (x\in A\wedge x\notin A)\vee(x\in A\wedge x\notin B)\}\\
&\Leftrightarrow x\in\{x\mid x\in A\wedge x\notin B\}\\
&\Leftrightarrow x\in A-B
\end{aligned}$$

定义 3.10 设 A,B 是两个集合。A 和 B 的对称差 $A\oplus B$ 就是

$$A\oplus B=\{x\mid x\in A\overline{\vee}x\in B\}$$

这里符号“$\overline{\vee}$”表示异或。因此，对称差的定义也可表示成

$$A\oplus B=\{x\mid x\notin A\rightleftarrows x\in B\}$$

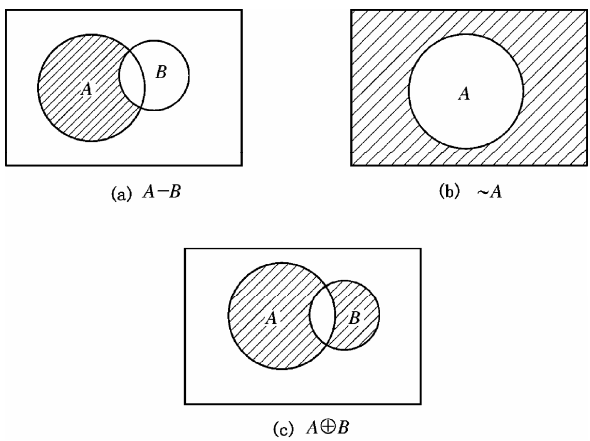
或

$$A\oplus B=\{x\mid x\in A\rightleftarrows x\notin B\}$$

或

$$A\oplus B=\{x\mid (x\notin A\wedge x\in B)\vee(x\in A\wedge x\notin B)\}$$

图 3.2 是差、补和对称差的文氏图。



(a) $A-B$　　(b) $\sim A$

(c) $A\oplus B$

图 3.2　差、补和对称差的文氏图

3.1.3　集合运算中的恒等式

在本章 3.1.2 节中通过集合的等式给出了一些关于集合运算的初等性质，实际上，那里出现的大部分公式（包括一些对任意集合证明的例题）都是恒等式。就是说，这些等式中的任何一个大写字母均可以用一个确定的集合替代，并且等式仍然成立。所以，这些等式中的大写字母可以看成是一个集合变量，类似于命题演算中的命题变元。

表 3.1 列出了有关集合的主要恒等式。

表 3.1　集合运算的基本恒等式

$A \cap A = A$ $A \cup A = A$	幂等律（1）
$\sim(\sim A) = A$	对合律（2）
$(A \cap B) \cap C = A \cap (B \cap C)$ $(A \cup B) \cup C = A \cup (B \cup C)$	结合律（3）
$A \cap B = B \cap A$ $A \cup B = B \cup A$	交换律（4）
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	分配律（5）
$A \cap (A \cup B) = A$ $A \cup (A \cap B) = A$	吸收律（6）
$\sim(A \cap B) = \sim A \cup \sim B$ $\sim(A \cup B) = \sim A \cap \sim B$	摩根律（7）
$A \cap \mathbf{E} = A$ $A \cup \varnothing = A$	同一律（8）
$A \cap \varnothing = \varnothing$ $A \cup \mathbf{E} = \mathbf{E}$	零一律（9）
$A \cap \sim A = \varnothing$ $A \cup \sim A = \mathbf{E}$	否定律（10）

注意表中隐含的两个本质属性。其一，以上这些公式如果其中含有交或并运算，则将这两个运算一次性地互换（即将“$\cap$”换成“$\cup$”，将“$\cup$”换成“$\cap$”），并将集合 $\mathbf{E}$ 和 $\varnothing$ 也互换，将得到另一等式，且它也是恒等式。这种成对的等式，通常叫做**对偶式**或简称为**偶式**。其二，将表 3.1 和第 2 章的表 2.14 比较一下，会发现它们之间惊人地类似。实际上，逻辑演算和集合演算在形式上的雷同，将在后面第 7 章中统一在布尔代数的同一理论框架之下。请读者在学完第 7 章之后，再返回到第 2 章和第 3 章来回味一下，那时，会有一种高屋建瓴之势。是的，谁能不折服于真正理论的严谨、概括、洗练和优美呢？

表 3.1 中每一恒等式都可以从相应的定义出发（前提），通过谓词演算的推理得到。以下是一个例子。

【例 3.7】　试证明表 3.1 中的吸收律。

证明　首先由分配律与幂等律有

$$A \cap (A \cup B) = (A \cap A) \cup (A \cap B) = A \cup (A \cap B)$$

于是只要证 $A \cap (A \cup B) = A$ 就行了。而

$$\begin{aligned} A \cap (A \cup B) &= (A \cup \varnothing) \cap (A \cup B) \\ &= A \cup (\varnothing \cap B) \\ &= A \cup \varnothing \\ &= A \end{aligned}$$

当然，我们也可以用谓词演算推理来证明吸收律。下面就是这样的证明。

$$A \cap (A \cup B) = \{x \mid x \in A \wedge (x \in A \vee x \in B)\}$$

$$= \{x \mid x \in A\}$$

$$= A$$

推导的第二步上，用了谓词演算中的吸收律。

应该指出，表 3.1 所列出的恒等式并不都是独立的。例 3.7 就说明这一点。实际上，只要其中少数几个就可以推出其余公式。这方面的内容将在第 7 章里会有进一步的论述。

3.1.4 序偶和笛卡儿积

现实世界中有许多事物是成对出现的，而且其中的两个事物有一定的次序。例如一双鞋有左右两只，一对父子，影剧院中一个座位按排号和列号对号入座，平面上的一点对应横坐标和纵坐标，空间中一点对应一组平面坐标和一个高度坐标（$<<x,y>,z>$），等等。概括起来说，数学上用两个有次序的元素组成一个称为**序偶**的结构，就可以表示客观世界中那种总是成对出现且具有一定次序的事物。

定义 3.11 设 A,B 是两个集合，对于 $a \in A$ 和 $b \in B$，有序集合 $<a,b>$ 叫做序偶。其中 a 叫做序偶的**第一元素**，b 叫做**第二元素**。

例如，某制鞋厂有某型号某尺码左脚鞋的生产线，它生产的鞋的集合用 L 表示。生产同型号同尺码右脚鞋的生产线的产品集合用 R 表示。若 $a \in L, b \in R$，那么序偶 $<a,b>$ 就表示一双鞋。又如果 $\mathbf{R}$ 表示实数的集合，$r_1 \in \mathbf{R}, r_2 \in \mathbf{R}$，那么 $<r_1, r_2>$ 就表示平面笛卡儿坐标上的一点。

三元组亦看成是序偶。一个三元组是由第一元素为序偶，第二元素是一般集合元素所组成的序偶，即

$$<a,b,c>=<<a,b>,c>$$

因此，$<a,<b,c>>$ 这样的序偶，在我们这里不是一个三元组，虽然它是一个序偶。

类似地，四元组被定义为一个三元组和一个集合元素的序偶等等。

定义 3.12 两序偶 $<a,b>, <c,d>$ 是相等的，当且仅当它们各自的第一元素和第二元素对应相等，即 $a=c, b=d$。

定义 3.13 设 A,B 是两个集合。所有由第一元素属于 A，第二元素属于 B 的序偶组成的集合叫做 A 与 B 的笛卡儿积。记为 $A \times B$，即

$$A \times B = \{<x,y> \mid x \in A, y \in B\}$$

我们约定，若两集合 A,B 中有一个（至少一个）为空集时，笛卡儿积 $A \times B = \varnothing$。

【例 3.8】 设 $A=\{1,2,3\}, B=\{a,b\}$，求 $A \times B$ 和 $B \times A$。

解 $A \times B = \{<1,a>,<1,b>,<2,a>,<2,b>,<3,a>,<3,b>\}$

$B \times A = \{<a,1>,<a,2>,<a,3>,<b,1>,<b,2>,<b,3>\}$

由上例可知，一般来说 $A \times B \neq B \times A$。所以说集合的笛卡儿积不满足交换律。因为笛卡儿积仍是一集合，所以可以求它与另一集合的积。例如 $(A \times B) \times C$ 或者 $A \times (B \times C)$。由于前一个积中的元素是三元组，而后一个积的元素不是三元组，所以它们一般情况下是不相等的，即集合的笛卡儿积不满足结合律。

定理 3.1 设 A,B,C 是任意给定的三个集合。则有

（a）$A \times (B \cap C) = (A \times B) \cap (A \times C)$ （3.27）

（b）$A \times (B \cup C) = (A \times B) \cup (A \times C)$ （3.28）

（c）$(A\cap B)\times C=(A\times C)\cap(B\times C)$ （3.29）

（d）$(A\cup B)\times C=(A\times C)\cup(B\times C)$ （3.30）

以上式（a）和（c）一起表达的是笛卡儿积对集合交的分配律，式（b）和（d）一起表达的是笛卡儿积对集合并的分配律。

我们选择（a）来证明之。

证明

$$\begin{aligned}A\times(B\cap C)&=\{<x,y>|\ x\in A\wedge(y\in B\wedge y\in C)\}\\&=\{<x,y>|\ (x\in A\wedge y\in B)\wedge(x\in A\wedge y\in C)\}\\&=\{<x,y>|\ (<x,y>\in A\times B)\wedge(<x,y>\in A\times C)\}\\&=\{<x,y>|<x,y>\in(A\times B)\cap(A\times C)\}\\&=(A\times B)\cap(A\times C)\end{aligned}$$

最后我们给出一个重要的约定。由于笛卡儿积不满足结合律，所以

$$A_1\times A_2\times A_3\equiv(A_1\times A_2)\times A_3$$

该集合是三元组的集合，而集合 $A_1\times(A_2\times A_3)$ 则不是三元组的集合。又

$$\begin{aligned}A_1\times A_2\times A_3\times A_4&\equiv(A_1\times A_2\times A_3)\times A_4\\&\equiv((A_1\times A_2)\times A_3)\times A_4\end{aligned}$$

一般的有

$$\begin{aligned}&A_1\times A_2\times A_3\times\cdots\times A_n\\&\equiv(A_1\times A_2\times\cdots\times A_{n-1})\times A_n\\&\equiv((A_1\times A_2\times\cdots\times A_{n-2})\times A_{n-1})\times A_n\\&\equiv(((A_1\times A_2\times\cdots\times A_{n-3})\times A_{n-2})\times A_{n-1})\times A_n\\&\equiv\cdots\\&\equiv(\cdots((A_1\times A_2)\times A_3)\cdots\times A_{n-1})\times A_n\end{aligned}\qquad(3.31)$$

3.2 关系

3.2.1 关系及其表示法

关系是现实世界中广泛存在着的概念。日常生活中有朋友关系、父子关系、买卖关系、债权和债务关系，等等，而各门学科中也存在函数关系、原函数与导数关系、对称关系、相似关系、同构关系，等等。实际上，从本节给出的最一般关系的概念出发，可以衍生出种种特定的关系。因此，给出关系最一般的定义显然对我们研究每一种特殊关系是很有好处的。事实上，关系的最一般的理论，可以适用于每一种特定的关系。例如，函数关系是一种特殊的关系。所以，一切关系的普遍规律对函数关系也是适用的。

现实世界中存在着各种各样的对象，可以是具体的如一个人、一辆车、一本书等等，也可以是一个抽象名词（概念）如实数、语言、战争、和平等等，客观世界正是由发展变化的事物组成的，而事物之间存在着一定的相互作用、相互联系和相互制约的关系。例如，表 3.2 给出了某些产品与生产该产品的厂家和使用它的厂家之间的联系。同一厂家可以生产不同的产品，同一产品也可由不同厂家生产。对使用厂家来说也有类似的关系。所以，一张像表 3.2 那样的二维表就完全地表达了一些产品与有关厂家的产销关系。通俗地讲，关系就是客观世

界一定范围的对象之间的某种特定联系。表中的每一行称为一个**实体**。它有三个属性，即生产厂家、产品和使用厂家。第一行中的属性名称也称**表目**。不同的行，表示不同的实体联系。它们都有三个相同的属性，只是属性的取值不同。表中所有实体就构成了一定范围的某些产品的产销关系。对于表中的每一行，容易想到的是用一个三元组来表示它，如 $<a_1,c_1,f_1>,<a_1,c_2,f_2>$ 等等。所以我们可以说，表中除表目以外的所有行对应的实体的集，就形象地表示了一个产销关系。以后在关系型数据库中会知道，这正是关系数据库的基础。

表 3.2　产品与生产厂家和使用厂家的联系

生产厂家	产品	使用厂家
a_1	c_1	f_1
a_1	c_2	f_2
a_1	c_3	f_1
a_2	c_2	f_1
a_3	c_1	f_2
a_3	c_3	f_2

下面从定义二元关系来开始我们的讨论。

那么从数学角度出发，表 3.2 又是什么呢？或者说如何以一种数学语言来描述这张表所给出的产销关系呢？实际上，从第 1 章绪论中的讨论可知，这就是如何建立起一个关系的数学模型的问题。

定义 3.14　设 A,B 是两个非空集合。笛卡儿积 $A\times B$ 的一个子集 $R\subseteq A\times B$，定义了一个从 A 到 B 的**二元关系**。并且，对于 $a\in A, b\in B$，如果 $<a,b>\in R$，则称元素 a 与 b 有关系 R，记为 aRb。否则，若 $<a,b>\notin R$，则 a 与 b 无关系 R，可记为 $a\overline{R}b$。特别当 $A=B$ 时，称 R 是 A 上的二元关系。

例如，有理数 $\mathbf{Q}$ 上的“小于等于”关系（就用符号“≤”表示这个关系）可记为

$$\leqslant=\{<x,y>\mid x,y\in\mathbf{Q}, x\leqslant y\}$$

注意上式中等号左边的“≤”并非按数学上通常理解的如式子“2≤3”里那样的符号。它实际上是一个集合的名字。在此，它表示“$\mathbf{Q}$ 上的小于等于关系”。而上式中第二个“≤”才是数学上普遍意义的符号。

定义 3.15　设 R 是 A 到 B 上的二元关系。一切属于关系 R 的序偶 $<x,y>\in R$ 中，第一元素 x 的集合，叫做 R 的**前域**，记为 dom$R$，即

$$\mathrm{dom}R=\{x\mid x\in A,(\exists y)(y\in B\wedge<x,y>\in R)\}$$

另外，一切属于 R 的序偶 $<x,y>\in R$ 中，第二元素 y 的集合叫做 R 的**值域**，记为 ran$R$，即

$$\mathrm{ran}R=\{y\mid y\in B,(\exists x)(x\in A\wedge<x,y>\in R)\}$$

【例 3.9】　令 $A=\{a,b,c\}$，$B=\{1,2,3,4\}$

$$R=\{<a,4>,<b,1>,<b,3>\}$$

于是

$$\mathrm{dom}\,R=\{a,b\},\mathrm{ran}\,R=\{1,3,4\}$$

注意到一个集合 A 到 B 的二元关系 R 的前域可以是 A 的真子集 $\mathrm{dom}\,R\subset R$，而值域也可是 B 的真子集 $\mathrm{ran}\,R\subset B$。本例的情况正是如此。

有限集合 A 到有限集合 B 的二元关系可以用一个所谓**关系图**的图形来表示它。我们可以

这样做：将各属于集合 A 和 B 的所有元素分别用两列点来表示。若 $x\in A$，$y\in B$，且 $<x,y>\in R$，那么，画一根以 x 为起点的有向弧指向 y。图 3.3 就是例 3.9 中的二元关系的关系图。

【例 3.10】 设 $A=\{2,3,6,8,12,32\}$。试写出 A 上的整除关系 D。

解 $D=\{<x,y>|\ x,y\in A, x\mid y\}$

$=\{<2,2>,<2,6>,<2,8>,<2,12>,<2,32>,$

$<3,3>,<3,6>,<3,12>,<6,6>,<6,12>,$

$<8,8>,<8,32>,<12,12>,<32,32>\}$

像例 3.10 那样在一个集合 A 上给出的关系，也可以用关系图来表示，不过这次我们可以在纸上按任意方式画出所有表示集合 A 中元素的点 *。当一个元素与它自己构成该关系的一对序偶时，则我们通过表示该元素的点画一个闭合的有向弧。至于该弧的方向沿顺时针还是逆时针是无关紧要的。图 3.4 给出了例 3.10 中的整除关系的关系图。

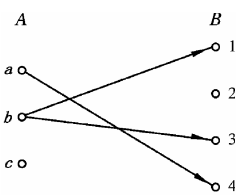


图 3.3　关系图的例子

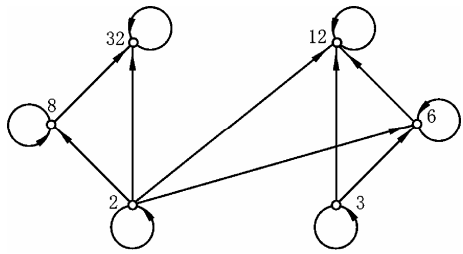


图 3.4　整除关系

关系的概念很容易推广至 n 元关系（n>2）的情况。

定义 3.16　设 $A_1, A_2, \cdots, A_n$ 是 n 个非空集合。$A_1\times A_2\times\cdots\times A_n$ 的任一子集 $R\subseteq A_1\times A_2\times\cdots\times A_n$，定义了一个集合 $A_1, A_2, \cdots, A_n$ 的 n 元关系。若对 $a_i\in A_i(i=1,2,\cdots,n)$，$n$ 元组 $<a_1,a_2,\cdots,a_n>\in R$，就说诸元素 $a_1, a_2, \cdots, a_n$ 之间存在 n 元关系 R。记为 $a_1a_2\cdots a_nR$。

表 3.2 给出的产销关系就是一个生产厂家、产品和使用厂家的三元关系。

一般而言，三元及三元以上关系不用关系图来表达。但是所有关系均可以用如表 3.2 那样的二维表来给出。通常关系数据库的教课书或文献中，就是用表来形象地给出一个关系数据库的。

表 3.3 中有 n 列，表目中的 n 项表示 n 个属性名，对应着定义 n 元关系的 n 个集合的名字 A_i。同一列中其余元素 a_{ij} 是属于集合 A_j 的一个元素。同一行中的 n 个元素 $a_{i1}, a_{i2}, \cdots, a_{in}$ 组成一个 n 元组，一般也叫**记录项**。表中没有重复的 n 元组。表中所有 n 元组的集合定义一个 n 元关系。

表 3.3　n 元关系的二维表

A_1	A_2	A_3	$\cdots$	A_n
a_{11}	a_{12}	a_{13}	$\cdots$	a_{1n}
a_{21}	a_{22}	a_{23}	$\cdots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{m1}	a_{m2}	a_{m3}	$\cdots$	a_{mn}

* 可是，循一定的规律安排这些点，可使画出的图更加简洁。参考上面的图 3.4。

本书主要讨论二元关系，以后不特别说明的话，当我们说关系一词时，指的就是二元关系。

非空的笛卡儿积 $A\times B$ 有两个平凡子集，它们是 $\varnothing$ 和 $A\times B$ 。$\varnothing$ 叫做**空关系**， $A\times B$ 叫做**全域关系**。例如， A 表示一家庭成员的集合，那么 A 上（ A 到 A ）的“不相识关系”是一个空关系，而“相识关系”是一个全域关系。

定义 3.17　设 I_A 是集合 A 上的二元关系。若 $I_A=\{<x,x>|\ x\in A\}$，则称 I_A 是 A 上的**恒等关系**。

例如，全体实数 $\mathbf{R}$ 上的相等关系是一个恒等关系。但是要注意，上面提到的家庭成员中的相识关系是全域关系，但不是恒等关系。

无论是关系图或二维表，都不便于对关系做数学处理。下面将引入一种既适于数学处理，又便于计算机存取的二元关系的表示方法，这就是二元关系的矩阵表示。

设已知两个有限集合 $A=\{a_1,a_2,\cdots,a_m\}$， $B=\{b_1,b_2,\cdots,b_n\}$ 。事先为每一集合中的元素任意约定一个次序。这种次序一经约定，在问题讨论结束之前就固定不变。

定义 3.18　设有有限集合 $A=\{a_1,a_2,\cdots,a_m\}$， $B=\{b_1,b_2,\cdots,b_n\}$ 。假设事先已为每一集合中所有元素各约定好一个次序。 $m\times n$ 矩阵 $\boldsymbol{M}_R=[r_{ij}]_{m\times n}$ 叫做 A 到 B 的关系 R 的关系矩阵，当且仅当

$$r_{ij}=\begin{cases}1 & \text{当}<a_i\ ,b_j>\in R\ (\text{或}a_iRb_j)\\ 0 & \text{否则}\end{cases}$$

其中 $1\leqslant i\leqslant m$,$1\leqslant j\leqslant n$ 。

一个 A 到 B 的空关系可用一个元素全为零的 $m\times n$ 矩阵表示，全域关系 $A\times B$ 的关系矩阵是全部元素为 1 的 $m\times n$ 矩阵，而 A 上的恒等关系则是一个主对角线全部为 1 的 $m\times m$ 方阵或者称单位矩阵。

【例 3.11】　给出例 3.10 中整除关系的关系矩阵。

解　例 3.10 中 A 的元素约定按升序排列，则它的关系矩阵是

$$\boldsymbol{M}_D=\begin{bmatrix}1&0&1&1&1&1\\0&1&1&0&1&0\\0&0&1&0&1&0\\0&0&0&1&0&1\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}$$

有必要指出，为了使关系矩阵唯一地与一个确定的二元关系对应，我们做了一个关于集合元素次序的约定。但是这种次序对一个关系不是本质的，它可以是任意的。换句话说，若我们改变了那个次序，即有限次交换集合中元素的位置，对同一关系而言，所得的关系矩阵虽不相同，但是你总可以从一个矩阵出发，相应地交换某些行（如交换了集合 A 中某两元素次序）或列（如交换了 B 中某两元素次序）而得到另一个矩阵。

3.2.2　几种特殊的关系

本小节将问题的讨论限制在 A 上的二元关系。

定义 3.19　设 R 是 A 上二元关系。若对任意 $x\in A$，都有 xRx，则称 R 是一个自反关系。

即

$$R\text{是自反的}\Leftrightarrow(\forall x)(x\in A\rightarrow xRx) \tag{3.32}$$

前面提到过的恒等关系 I_A 是一种特殊的自反关系。但是，自反关系不必是恒等关系。例如，实数集的“小于等于”关系就是自反关系。

属于自反关系的还可以举出很多例子，如集合 C 的幂集 $\rho(C)$ 上的“包含于”关系，全体平面图形的相似关系等等。

有一个很重要的自反关系，就是整数集 $\mathbf{Z}$ 上的**模 k 同余关系**。模数 k 是一个大于 1 的正整数。对于整数 $a\in\mathbf{Z}$，总有唯一的等式

$$a=kq+r$$

且其中 $0\leqslant r<k$。于是我们说 a 有模 k 余数 r 。记做 $a(\mathrm{mod}\,k)=r$ 。

例如， $k=3$ 。那么 $7(\mathrm{mod}\,3)=1$， $5(\mathrm{mod}\,3)=2$， $-5(\mathrm{mod}\,3)=1$（注意不等于-2，因为要求 $r\geqslant 0$）。

如果两个整数 $z_1,z_2\in\mathbf{Z}$ 的模 k 余数相等，我们就说它们有**模 k 同余关系**，并记为 $a=b(\mathrm{mod}\,k)$ 。

【例 3.12】 证明整数 $\mathbf{Z}$ 上的模 k（$k\in\mathbf{Z},k>1$）同余是自反关系。

证明 任取一个整数。 $a\in\mathbf{Z}$，显然 $a(\mathrm{mod}\,k)=a(\mathrm{mod}\,k)$，即 a 与 a 有模 k 同余关系。

定义 3.20 设 R 是 A 上二元关系。如果对任意 $a,b\in A$，当有 aRb 则必有 bRa，就称 R 是一个**对称关系**。即

$$(\forall x)(\forall y)((x\in A\wedge y\in A\wedge xRy)\rightarrow yRx) \tag{3.33}$$

对称关系是一种比较常见的二元关系。例如，一群人之中的“朋友关系”是对称的。各种领域内的“相等”、“对称”和“互补”关系都是对称的。

例如，全集 $\mathbf{E}$ 上两集合 X,Y 有补关系，说的是它们满足 $X\cup Y=\mathbf{E}$ 和 $X\cap Y=\varnothing$。显然，补关系是对称的。补关系的对称性，源于集合的交和并运算是可交换的。

定义 3.21 设 R 是 A 上二元关系，对于 $x,y,z\in A$，若 xRy 和 yRz 就必有 xRz，则称关系是**可传递的**。即

$$(\forall x)(\forall y)(\forall z)((x\in A\wedge y\in A\wedge z\in A\wedge xRy\wedge yRz)\rightarrow xRz) \tag{3.34}$$

实数上的小于等于关系，几何上的相似关系，集合的包含（于）关系，都是可传递关系。但人际间的“朋友关系”未必是可传递的。

定义 3.22 设 R 是 A 上二元关系。对于 $x,y\in A$，若有 xRy,yRx，则必定有 $x=y$，称 R 是**反对称关系**。即

$$(\forall x)(\forall y)((x\in A\wedge y\in A\wedge xRy\wedge yRx)\rightarrow(x=y)) \tag{3.35}$$

一种与上式等价的表达为我们提供了从另一角度理解反对称关系的可能（参考例 2.21 的等价关系）。它是

$$(\forall x)(\forall y)((x\in A\wedge y\in A\wedge(x\neq y)\wedge xRy)\rightarrow(y\ \overline{R}\ x))$$

其中符号“$y\overline{R}x$”表示“y 和 x 没有关系 R”。这就是说，对一个反对称关系来说，任何两个不相等的元素之间不存在“对称”的关系（即不可能 xRy 和 yRx 同时成立）。

人群中的父子关系，实数上的“小于”或“小于等于”关系，整除关系，集合中的包含关系等，都是反对称的关系。建议读者特别地把“小于”是反对称关系的道理弄明白。

为了更好地理解这些定义，我们来进一步剖析一下式（3.32），式（3.33），式（3.34）和式（3.35）。它们有以下三种类型：

$$(\forall x)P(x)$$
$$(\forall x)(\forall y)Q(x,y)$$
$$(\forall x)(\forall y)(\forall z)R(x,y,z)$$

其中 $P(x),Q(x,y),R(x,y,z)$ 是谓词公式。这些式子的否定形式分别是

$$\neg\ (\forall x)P(x) \Leftrightarrow (\exists x)\neg\ P(x)$$
$$\neg\ (\forall x)(\forall y)Q(x,y) \Leftrightarrow (\exists x)\neg\ (\forall y)Q(x,y)$$
$$\Leftrightarrow (\exists x)(\exists y)\neg\ Q(x,y)$$
$$\neg\ (\forall x)(\forall y)(\forall z)R(x,y,z) \Leftrightarrow (\exists x)\neg\ (\forall y)(\forall z)R(x,y,z)$$
$$\Leftrightarrow (\exists x)(\exists y)\neg\ (\forall z)R(x,y,z)$$
$$\Leftrightarrow (\exists x)(\exists y)(\exists z)\neg\ R(x,y,z)$$

由此可见，只要有一个元素 x（或一对元素 x,y，或一组元素 x,y,z）令谓词公式 $P(x)$（或 $Q(x,y)$，或 $R(x,y,z)$）为假，就是说找到一处不符合定义的情况，该定义就不成立，或者说，被验证的关系不具有该定义所描述的性质。

例如，设 $A=\{a,b,c\},R=\{<a,a>,<a,b>\}$。初学者往往肯定 R 是自反的，其理由是 aRa，并说成“a 是自反的”。事实上由于 $b\overline{R}b$（甚至不必再提到还有 $c\overline{R}c$）就可知 R 在 A 上不是自反的。

另一种极端是将符合某定义的关系说成是不具有定义给出的性质。

例如，设 $A=\{a,b,c\},R=\{<a,b>\}$。这是 A 上的一个传递关系。关于这一点，如果读者感到大惑不解的话，可以自问一下：“关系 R 是否真不符合式（3.34）给出的定义呢?”问题出现了，归根结底还是一种对蕴含形式给出的命题 $P\rightarrow Q$ 的不正确理解。$P\rightarrow Q$ 为真，要求的是对假设前提为真时，结论 Q 一定为真。除此之外，它并不理会别的什么。反过来说，要证实 $P\rightarrow Q$ 不是真的，只能通过举一个反例的方法才成，即找出一种情况，这时 P 成立（为真），而 Q 不成立（为假）。那么，在刚才的例子里，$R=\{<a,b>\}$，能找到这样三个元素 $x\in A,y\in A,z\in A$，使 xRy 和 yRz 都成立吗？不能，这就是说，既然举不出一种假设前提为真的情况，又如何去论证 $P\rightarrow Q$ 为假的呢？于是又回到过去讲过的“善意推断”。

从关系 R 的关系矩阵 $\boldsymbol{M}_R$ 和关系图可以容易地判断 R 的某些性质。

1．关系 R 是自反的，当且仅当 $\boldsymbol{M}_R$ 的主对角线上的元素全为 1，关系图每个结点上都有一条自闭合的有向弧。

2．R 是对称的，当且仅当 $\boldsymbol{M}_R$ 是对称矩阵，关系图上不同两点间如果有有向弧，则两点间的有向弧必是一对方向相反的。

3．R 是反对称的，当且仅当 $\boldsymbol{M}_R$ 中关于主对角线对称的两元素不会同时都为 1，关系图中不同两点间不存在成对的、方向相反的有向弧。

4．R 是传递的，如果其关系图中存在任意由两条或两条以上的有向弧沿同一方向连续连接成的弧线，则必有从该弧线的起点至它的终点的有向弧，若该弧线是闭合的，则在起点（也是终点）上，有一条自闭合的有向弧。从而，该闭合弧线的每一个结点上存在一个自闭合的有向弧。

稍后给出通过矩阵判别传递性的方法。

对一个建立在两个不同集合 B 到 C 上的二元关系 R，我们可以令 $A=B\cup C$。显然，R 也就成了 A 上的二元关系。当然，如果 $B\cap C=\varnothing$，则在集合 $A=B\cup C$ 上定义的这个关系 R 不可能是自反的、对称的，但一定是传递的和反对称的。想想看，为什么？

3.2.3 关系的运算

1．关系的交、并、差、补

设 R 和 S 是集合 A 到 B 的二元关系，则可证 R 和 S 的交、并、差和 R 或 S 的补都是 $A\times B$ 的子集。因此，按照二元关系的定义，它们都仍然是 A 到 B 的二元关系。即

$$R\cap S\subseteq A\times B,\quad R\cup S\subseteq A\times B,\quad R-S\subseteq A\times B$$

再若我们令 $A\times B$（全域关系）作为讨论 A 到 B 的一切关系的完全集，那么 R 和 S 的补集

$$\sim R=(A\times B)-R\subseteq A\times B,\quad \sim S=(A\times B)-S\subseteq A\times B$$

定理 3.2 设 R,S 都是集合 A 到 B 的二元关系，则 $R\cap S$，$R\cup S$，$R-S$ 和 $\sim S$ 都是 A 到 B 的二元关系。

证明 由关系的定义 3.14 可知，只要证明 R 和 S 的运算结果是 $A\times B$ 的子集就行了。以 $R-S$ 和 $\sim R=(A\times B)-R$ 为例。

先证 $R-S\subseteq A\times B$。

事实上，任取 x,y，设 $<x,y>\in R-S$，

$$<x,y>\in R-S\Leftrightarrow(<x,y>\in R)\wedge\neg\ (<x,y>\in S)$$
$$\Rightarrow<x,y>\in R\Rightarrow<x,y>\in A\times B$$

即得 $R-S\subseteq A\times B$。

又设 $<x,y>\in\sim R$，则

$$<x,y>\in\sim R\Leftrightarrow<x,y>\in(A\times B)-R$$
$$\Leftrightarrow(<x,y>\in A\times B)\wedge\neg\ (<x,y>\in R)$$
$$\Rightarrow<x,y>\in A\times B$$

于是 $\sim R\subseteq A\times B$。

【例 3.13】 A 是某学习班学生的集合。R,S 是 A 上的两个关系：

$$R=\{<x,y>\mid x\in A,y\in A,x\text{ 与 }y\text{ 是同姓氏的}\}$$
$$S=\{<x,y>\mid x\in A,y\in A,x\text{ 与 }y\text{ 是同乡}\}$$

试问关系 $R\cap S,R\cup S,R-S,S-R,\sim R,\sim S$ 各有何含义？

解 $R\cap S$ 表示班级 A 上学生间既是同姓又是同乡的关系。

$R\cup S$ 表示 A 上是同姓的或者是同乡的关系。

$R-S$ 表示学生间是同姓而不是同乡的关系。

$S-R$ 表示学生间是同乡而不是同姓的关系。

$\sim R$ 表示不同姓关系。

$\sim S$ 表示不是同乡的关系。

2．关系的复合

正如数学分析中所知，两个函数 $f(x),g(x)$ 在一定条件下可以施行复合，形成新的复合函数那样，两个关系在一定条件下也可以复合成新关系。

定义 3.23 设 A,B,C 是三个非空集合，而 R 是 A 到 B 的二元关系，S 是 B 到 C 的二元关系。则符号 $R\circ S$ 表示 R 和 S 的复合，即

$$R \circ S = \{< x,z > \mid x \in A \wedge z \in C \wedge (\exists y)(y \in B \wedge xRy \wedge ySz)\} \tag{3.36}$$

显然，$R \circ S$ 是一个 A 到 C 的关系。我们约定，若 R 或 S 之一为空关系，则 $R \circ S$ 亦为空关系。

关系的复合的概念可以推广到多于 2 个关系的情形。设 A, B, C, D 是四个集合。R, S, W 分别是 A 到 B，B 到 C 和 C 到 D 的关系。则 $(R \circ S)$ 是 A 到 C 的关系，所以进而可以有 $(R \circ S) \circ W$，最后复合成一个 A 到 D 的关系。自然会想到，$R \circ (S \circ W)$ 也是 A 到 D 上的关系。那么，是否由于复合的次序不同而使所得的两个复合关系不相等呢？回答是否定的。即有

$$(R \circ S) \circ W = R \circ (S \circ W) \tag{3.37}$$

事实上，设 R, S, W 均非空，并有 $x((R \circ S) \circ W)w$，即 $< x,w > \in (R \circ S) \circ W$。那么，必有 $< x,z > \in R \circ S$ 和 $< z,w > \in W$。也即有 $< x,y > \in R$ 和 $< y,z > \in S$ 以及 $< z,w > \in W$。进而有 $< x,y > \in R$ 和 $< y,w > \in S \circ W$，所以 $< x,w > \in R \circ (S \circ W)$。反之，也可证明若 $< x,w > \in R \circ (S \circ W)$，则 $< x,w > \in (R \circ S) \circ W$。

再若 R, S, W 之中有一为空关系，则式（3.37）两侧均为空关系。所以式（3.37）恒成立。以上公式（3.37）表示关系的复合运算满足结合律。

【例 3.14】 设 $A = \{a_1, a_2, a_3, a_4, a_5\}$，$B = \{b_1, b_2, b_3\}$，$C = \{c_1, c_2, c_3, c_4\}$。$A$ 到 B 的关系

$$R = \{< a_1, b_1 >, < a_1, b_3 >, < a_3, b_2 >, < a_3, b_3 >, < a_5, b_2 >, < a_5, b_3 >\}$$

B 到 C 的关系

$$S = \{< b_1, c_4 >, < b_2, c_1 >, < b_2, c_3 >, < b_3, c_1 >\}$$

求复合关系 $R \circ S$。

解 $R \circ S = \{< a_1, c_4 >, < a_1, c_1 >, < a_3, c_1 >, < a_3, c_3 >, < a_5, c_1 >, < a_5, c_3 >\}$

图 3.5 是关系 R 和 S 复合的示意图。

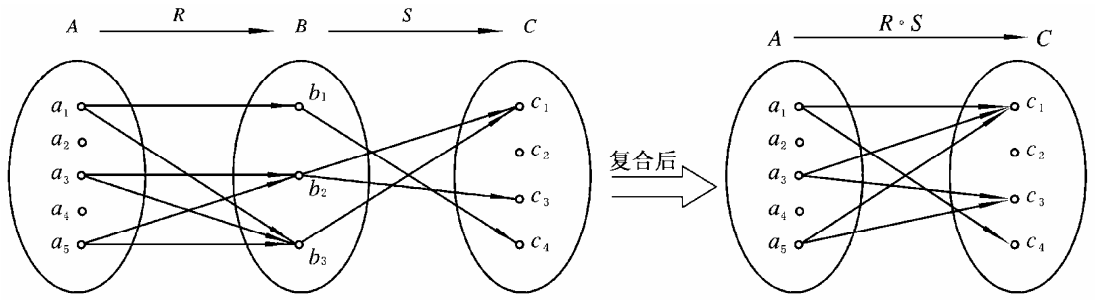


图 3.5　$R \circ S$ 的关系图

我们知道，集合 $A = \{a_1, a_2, \cdots, a_m\}$ 到 $B = \{b_1, b_2, \cdots, b_n\}$ 的关系 R 的关系矩阵 $\boldsymbol{M}_R = [u_{ij}]$ 是 $m \times n$ 阶的，而 B 到 $C = \{c_1, c_2, \cdots, c_r\}$ 的关系 S 的关系矩阵 $\boldsymbol{M}_S = [v_{jk}]$ 是 $n \times r$ 阶的，且关系矩阵中的每一个元素是 0 或者 1。按代数中矩阵相乘的定义，可以进行 $\boldsymbol{M}_R \times \boldsymbol{M}_S$，姑且用 $\boldsymbol{M}_{RS} = [w'_{ik}]$ 表示它们的积（而我们以 $\boldsymbol{M}_{R \circ S} = [w_{ik}]$ 表示 $R \circ S$ 的关系矩阵）。$\boldsymbol{M}_{RS}$ 是一个 $m \times r$ 阶矩阵，有

$$\begin{aligned} w'_{ik} &= u_{i1} \cdot v_{1k} + u_{i2} \cdot v_{2k} + \cdots + u_{in} \cdot v_{nk} \\ &= \sum_{j=1}^{n} (u_{ij} \cdot v_{jk}) \end{aligned} \tag{3.38}$$

其中 $1 \leqslant i \leqslant m$，$1 \leqslant k \leqslant r$。

设若有$b_{j_1},b_{j_2},\cdots,b_{i_t}\in B$，使$<a_i,b_{j_1}>,<a_i,b_{j_2}>,\cdots,<a_i,b_{j_t}>\in R$和$<b_{j_1},c_k>,<b_{j_2},c_k>,\cdots,<b_{j_t},c_k>\in S$，即$u_{ij_1}=u_{ij_2}=\cdots=u_{ij_t}=1$和$v_{j_1k}=v_{j_2k}=\cdots=v_{j_tk}=1$。上面公式（3.38）的和式里有$t$项等于 1，矩阵$\boldsymbol{M}_{RS}$中元素$w'_{ik}=t$。另一方面，由复合关系定义可知，这时必有$<a_i,c_k>\in R\circ S$。就是说，关系$R\circ S$的关系矩阵中相应位置上的元素$w_{ik}$应当是 1。将两个关系$R$和$S$的关系矩阵$\boldsymbol{M}_R$和$\boldsymbol{M}_S$按普通矩阵乘法的规则求出积$\boldsymbol{M}_{RS}=\boldsymbol{M}_R\times\boldsymbol{M}_S$，并且将它中间一切大于 0 的元素均以 1 取代后，$\boldsymbol{M}_{RS}$就成为复合关系$R\circ S$的关系矩阵$\boldsymbol{M}_{R\circ S}$（在阅读以上一段文字时，请注意$\boldsymbol{M}_{RS}$和$\boldsymbol{M}_{R\circ S}$两者的区别）。

有一种更直接的求$R\circ S$的关系矩阵的方法。这需要做一些约定。约定关系矩阵中的 0 和 1 一律看成是逻辑量 **F** 和 **T**。于是满足算律

$$0\wedge 0=0，\ 0\wedge 1=1\wedge 0=0，\ 1\wedge 1=1$$

$$1\vee 1=1，\ 1\vee 0=0\vee 1=1，\ 0\vee 0=0$$

回到前面关于两个关系矩阵$\boldsymbol{M}_R3$与$\boldsymbol{M}_S$的普通乘法的讨论，若将式（3.38）中的乘法“.”一律代之以逻辑乘“∧”，那里的加法“+”一律代之以逻辑加“∨”，即

$$w_{ik}=\bigvee_{j=1}^{n}(u_{ij}\wedge v_{jk}) \tag{3.39}$$

容易明白，这样得到的就是$R\circ S$的关系矩阵。用$\boldsymbol{M}_R\circ\boldsymbol{M}_S$表示式（3.39）给出的按逻辑算律所得矩阵的布尔积，终于有（用矩阵的逻辑乘算符“∘”代替它的代数乘算符“×”）

$$\boldsymbol{M}_R\circ\boldsymbol{M}_S=\boldsymbol{M}_{R\circ S} \tag{3.40}$$

这就是以下的定理：

定理 3.3 设$\boldsymbol{M}_R$是集合A到B的关系R的关系矩阵，$\boldsymbol{M}_S$是B到C的关系S的关系矩阵，则复合关系$R\circ S$的关系矩阵$\boldsymbol{M}_{R\circ S}$是按逻辑算律的$\boldsymbol{M}_R$与$\boldsymbol{M}_S$的积（布尔积）。

在例 3.14 中，有

$$\boldsymbol{M}_R=\begin{bmatrix}1&0&1\\0&0&0\\0&1&1\\0&0&0\\0&1&1\end{bmatrix}\qquad \boldsymbol{M}_S=\begin{bmatrix}0&0&0&1\\1&0&1&0\\1&0&0&0\end{bmatrix}$$

$$\boldsymbol{M}_{R\circ S}=\boldsymbol{M}_R\circ\boldsymbol{M}_S=\begin{bmatrix}1&0&0&1\\0&0&0&0\\1&0&1&0\\0&0&0&0\\1&0&1&0\end{bmatrix}$$

这里得出的$R\circ S$关系矩阵确实与例 3.14 中的答案是吻合的。

上一节中我们遗留下一个问题，就是如何利用集合A上关系R的关系矩阵$\boldsymbol{M}_R$来判断R是否传递的问题。现在就来继续这个讨论。

首先，设关系矩阵的元素 0 和 1 有关系：

$$0\leqslant 0，\ 1\leqslant 1，\ 0<1（1>0）$$

其次，约定A上的关系R,S的关系矩阵$\boldsymbol{M}_R=[u_{ij}]_{n\times n},\boldsymbol{M}_S=[v_{ij}]_{n\times n}$之间“小于等于”关系是

$$\boldsymbol{M}_R\leq\ \boldsymbol{M}_S\Leftrightarrow(\forall i)(\forall j)((1\leqslant i\leqslant n)\wedge(1\leqslant j\leqslant n)\wedge(u_{ij}\leqslant v_{ij}))$$

于是由集合的包含和关系矩阵的定义可知

$$R\subseteq S\Leftrightarrow\boldsymbol{M}_R\leq\ \boldsymbol{M}_S$$

考虑本章练习题 3.30 的结果，即设 R 是集合 A 上的二元关系， R 是传递的，当且仅当 $R\circ R\subseteq R$。所以，要判断 R 是否是传递的，只要证明其关系矩阵满足 $\boldsymbol{M}_{R\circ R}=\boldsymbol{M}_R\circ\boldsymbol{M}_R\leq\boldsymbol{M}_R$ 即可。

最后，作为一个练习，请读者证明关系的复合不满足交换律，即 $R\circ S\neq S\circ R$。

【例 3.15】 设有一组嵌套调用的函数是 $P_1(x_{11},x_{12},\cdots,x_{1r};a_{11},a_{12},\cdots,a_{1m})$， $P_2(x_{21},x_{22},\cdots,x_{2s};a_{21},a_{22},\cdots,a_{2n})$， $P_3(x_{31},x_{32},\cdots,x_{3t};a_{31},a_{32},\cdots,a_{3l})$，其中 x_{ij} 表示形参， a_{ij} 表示局部变量。试问，当用 r 个实参 $c_1,c_2,\cdots,c_r$ 对 P_1 调用后，诸函数中的哪些局部变量将会因 $c_1,\cdots,c_r$ 的值而发生变化？

解 为使讨论不致过于复杂，假设每一函数中不含有其他子函数或子过程调用 *。对于每一个函数 $P_i(i=1,2,3)$ 建立由各自形参的集合 X_i 到其局部变量的集合 A_i 的一个二元关系 $R_i=\{<x_{ij},a_{ik}>|\,x_{ij}\in X_i,a_{ik}\in A_i$，程序 P_i 中含有这样的赋值语句：由含有 x_{ij} 的表达式直接或间接对局部变量 a_{ik} 有效赋值$\}$。

另外，对每一层调用（ P_1 调用 P_2，P_2 调用 P_3），各建立一个由 P_i 中的局部变量集合 $A_i(i=1,2)$ 到程序 P_{i+1} 的形参集合 X_{i+1} 的二元关系

$$S_i=\{<a_{ik},x_{(i+1)j}>|\,a_{ik}\in A_i,x_{(i+1)j}\in X_{i+1},a_{ik}\text{ 调用 }P_{i+1}\text{ 的形参 }x_{(i+1)j}\}$$

最后算出以下所有二元关系及复合关系：

$$R_1,\ R_1\circ S_1\circ R_2,\ R_1\circ S_1\circ R_2\circ S_2\circ R_3$$

于是，所有上述关系中出现的序偶的第二元素（各程序中的局部变量）将可能会因调用 P_1 的诸实参的改变而改变。

3．逆关系

将集合 A 到 B 的关系 R 包含的每一序偶的两元素交换次序后，一般都得到一个 B 到 A 的新关系。后者就是关系 R 的**逆关系**，简称 R 的**逆**。记为 R^c。例如，父子关系的逆是子亲关系，“≤”关系的逆是“≥”关系，笛卡儿平面坐标上的直线 $L=\{<x,y>|\,ax+by+c=0,a,b\in\mathbf{R},\text{a·b}\neq 0,x,y\in\mathbf{R}\}$（其中 $\mathbf{R}$ 在此表示实数集合）的逆 $L^c=\{<y,x>|\,ay+bx+c=0,a,b\in\mathbf{R},\text{a·b}\neq 0,x,y\in\mathbf{R}\}$表示关于坐标系主角平分线（过原点平分第Ⅰ,Ⅲ象限的直线） L 的对称直线。

定义 3.24 设 R 是 A 到 B 的二元关系，对调属于 R 的一切序偶的两元素的次序，所得 B 到 A 的关系叫做 R 的逆关系，或简称 R 的逆，记作 R^c。即

$$R^c=\{<y,x>|\,x\in A,y\in B,<x,y>\in R\}\qquad(3.41)$$

容易明白 R^c 的关系图可由 R 的关系图逆转每一有向弧得到，而 R^c 的关系矩阵 $\boldsymbol{M}_{R^c}$ 恰为 R 的矩阵 M_R 的转置：

$$\boldsymbol{M}_{R^c}=(\boldsymbol{M}_R)^{\mathrm{T}}\qquad(3.42)$$

关于复合关系的逆的矩阵，有以下定理：

定理 3.4 设 A 到 B 有关系 R， B 到 C 有关系 S，那么复合关系 $R\circ S$ 的逆等于 $S^c\circ R^c$。即

$$(R\circ S)^c=S^c\circ R^c\qquad(3.43)$$

---

* 如果有子调用，一概假设为赋值调用。

证明　只要证明 $(R\circ S)^c \subseteq S^c \circ R^c$ 和 $S^c \circ R^c \subseteq (R\circ S)^c$。

任给 $z\in C, x\in A$。假设

$$<z,x>\in (R\circ S)^c$$

$$\Leftrightarrow <x,z>\in R\circ S \qquad \text{（逆的定义）}$$

$$\Leftrightarrow <x,z>\in \{<x,z>\mid x\in A, z\in C, (\exists y)(y\in B \wedge <x,y>\in R \wedge <y,z>\in S)\}$$

（复合关系定义）

$$\Leftrightarrow <z,x>\in \{<z,x>\mid x\in A, z\in C, (\exists y)(y\in B \wedge <y,x>\in R^c \wedge <z,y>\in S^c)\}$$

（逆的定义）

$$\Leftrightarrow <z,x>\in S^c\circ R^c \qquad \text{（复合关系定义）}$$

注意：$S^c\circ R^c$ 是一个集合 C 到 A 上的关系。

由于推论每一步都是等价的，证完。

【例 3.16】　求例 3.14 中关系 R, S 的逆，并由此验证公式（3.43）。

解　用关系矩阵表达是

$$M_{R^c}=(M_R)^{\mathrm{T}}=\begin{bmatrix}1&0&1\\0&0&0\\0&1&1\\0&0&0\\0&1&1\end{bmatrix}^{\mathrm{T}}=\begin{bmatrix}1&0&0&0&0\\0&0&1&0&1\\1&0&1&0&1\end{bmatrix}$$

$$M_{S^c}=(M_S)^{\mathrm{T}}=\begin{bmatrix}0&0&0&1\\1&0&1&0\\1&0&0&0\end{bmatrix}^{\mathrm{T}}=\begin{bmatrix}0&1&1\\0&0&0\\0&1&0\\1&0&0\end{bmatrix}$$

求 $(R\circ S)^c$。一方面有

$$M_{(R\circ S)^c}=(M_{R\circ S})^{\mathrm{T}}=\begin{bmatrix}1&0&0&1\\0&0&0&0\\1&0&1&0\\0&0&0&0\\1&0&1&0\end{bmatrix}^{\mathrm{T}}=\begin{bmatrix}1&0&1&0&1\\0&0&0&0&0\\0&0&1&0&1\\1&0&0&0&0\end{bmatrix}$$

另一方面

$$M_{S^c\circ R^c}=M_{S^c}\circ M_{R^c}=\begin{bmatrix}1&0&1&0&1\\0&0&0&0&0\\0&0&1&0&1\\1&0&0&0&0\end{bmatrix}$$

两种方法得到的结果当然是相同的。

还有一些有关逆的重要的恒等式：

$$(R\cup S)^c=R^c\cup S^c \qquad (3.44)$$

$$(R\cap S)^c=R^c\cap S^c \qquad (3.45)$$

$$(R-S)^c=R^c-S^c \qquad (3.46)$$

$$(\sim R)^c=\sim (R^c) \qquad (3.47)$$

以上 4 个公式，请读者作为练习完成它们的证明。

4．关系的闭包运算

将这一段讨论仅限于 A 上的二元关系。

关系的闭包运算就是在一个关系 R 中尽可能少地添补一些序偶，以使新的关系满足某一特殊性质的过程。

定义 3.25 设 R 是集合 A 上的二元关系，R' 也是 A 上的二元关系。R' 称为 R 的自反闭包，当且仅当（1）R' 是自反的，（2）$R' \supseteq R$，（3）任何 A 上的二元关系 $R'' \supseteq R$，若 R'' 是自反的，则 $R'' \supseteq R'$。

R 的自反闭包记为 $r(R)$。从定义的性质（3）可知，$r(R)$ 是一切包含 R 而且自反的关系中“最小的”一个。显然，若 R 是自反的，则 $r(R)=R$。反之亦然。

定义 3.26 设 R 是 A 上二元关系，R' 也是 A 上的二元关系。R' 称为 R 的对称闭包，当且仅当（1）R' 是对称的，（2）$R' \supseteq R$，（3）任何 A 上的二元关系 $R'' \supseteq R$，若 R'' 是对称的，则 $R'' \supseteq R'$。

R 的对称闭包记为 $s(R)$。

定义 3.27 设 R 是 A 上二元关系，R' 也是 A 上的二元关系。R' 称为 R 的传递闭包，当且仅当（1）R' 是传递的，（2）$R' \supseteq R$，（3）任何 A 上的关系 $R'' \supseteq R$，若 R'' 是传递的，则 $R'' \supseteq R'$。

R 的传递闭包记为 $t(R)$。

以下是有关求 R 的闭包的定理：

定理 3.5 设 R 是 A 上的二元关系。则

$$r(R) = R \cup I_A \tag{3.48}$$

其中 I_A 是 A 上恒等关系。

证明 令 $R' = R \cup I_A$

（1）由本章 3.1.2 节中公式（3.18）可知，$R' \supseteq R$。

（2）同理，$I_A \subseteq R'$。任取 $x \in A$，因为 $<x,x> \in I_A$，所以 $<x,x> \in R'$，即 R' 是自反的。

（3）设 A 上二元关系 R'' 是自反的，且 $R'' \supseteq R$。任取 $<x,y> \in R'$，有

$$\begin{aligned} <x,y> \in R' &\Leftrightarrow <x,y> \in R \cup I_A \\ &\Leftrightarrow <x,y> \in R \vee <x,y> \in I_A \end{aligned}$$

以上面最后这个析取式作为前提之一，结合假设 $R'' \supseteq R$，即 $<x,y> \in R \rightarrow <x,y> \in R''$ 和 R'' 是自反的，即 $<x,y> \in I_A \rightarrow <x,y> \in R''$ 这两个前提，再用第 2 章表 2.15 中式（11'），可知它们共同蕴含 $<x,y> \in R''$。由此证得：$R' \subseteq R''(R'' \supseteq R')$。

定理 3.6 设 R 是 A 上二元关系，则它的对称闭包是

$$s(R) = R \cup R^c \tag{3.49}$$

在给出传递闭包的定理之前，我们先约定一些记号。设 R 是 A 上的二元关系。R 自身的多次复合记为

$$R \circ R = R^{(2)}, R \circ R \circ R = R^{(3)}, \underbrace{R \circ R \circ \cdots \circ R}_{n\text{个}} = R^{(n)}$$

这里将 R 右上方的“指数”用括号封闭起来，是为了不与 R 的笛卡儿积相混淆。由于复合运算有结合律，所以 $R \circ R \circ R = R^{(2)} \circ R = R \circ R^{(2)} \cdots$

另外还约定

$$R^+ = R \cup R^{(2)} \cup \cdots \cup R^{(i)} \cup \cdots$$

通常，当集合 A 是无限集时，R^+ 不一定可以通过有限次运算得出。但是，当 A 为有限集时，R^+ 的确可通过有限次运算得到确定的值。

定理 3.7 设 R 是 A 上的二元关系。则它的传递闭包是

$$t(R) = R^+ = R \cup R^{(2)} \cup \cdots \tag{3.50}$$

证明

（1）证 R^+ 是传递的。

设有 $<x,y>,<y,z> \in R^+$，由式（3.50）可知，必有正整数 i，j，使 $<x,y> \in R^{(i)}$ 和 $<y,z> \in R^{(j)}$。由复合关系之定义可知

$$<x,z> \in R^{(i)} \circ R^{(j)} = R^{(i+j)} \subseteq R^+$$

（2）由式（3.50）直接可得 $R^+ \supseteq R$。

（3）设还有包含 R 的可传递关系 R''，来证明有 $R'' \supseteq R^+$。

任取 $<x,y> \in R^+$，即有正整数 i 使得 $<x,y> \in R^{(i)}$。当 $i \geqslant 2$，由复合关系定义可知，存在 $c_1, c_2, \cdots, c_{i-1} \in A$，使得 $<x,c_1> \in R, <c_1,c_2> \in R, \cdots, <c_{i-2},c_{i-1}> \in R$ 和 $<c_{i-1},y> \in R$。按假设 $R'' \supseteq R$，所以 $<x,c_1> \in R'', <c_1,c_2> \in R'', \cdots, <c_{i-2},c_{i-1}> \in R'', <c_{i-1},y> \in R''$。还因假设 R'' 是可传递的，最后有 $<x,y> \in R''$。当 i=1，直接有 $<x,y> \in R$，所以也有 $<x,y> \in R''$。即 $R'' \supseteq R^+$。

定理 3.8 设 $A = \{a_1, a_2, \cdots, a_n\}$ 为一有限集合，R 是 A 上二元关系。则存在正整数 $k \leqslant n$，使得

$$R^+ = R \cup R^{(2)} \cup \cdots \cup R^{(k)} \tag{3.51}$$

假设 R 是一个人群 A 上的关系，若 $u \in A, v \in A, <u,v> \in R$，表示 u 可与 v 单方联系。一般情况下这不是传递的关系。即，对于 $u \in A, v \in A$，即使有 $w \in A$，使得 $<u,w> \in R$ 和 $<w,v> \in R$，但是 $<u,v> \notin R$。可是，显然 $<u,v> \in R^{(2)}$。这可以解释为 u 对于 v 不能直接联系，却可以通过一个人 w 传递消息。而 $R^{(2)}$ 包含了所有像 u，v 这样的即使不能直接传递消息，但是可以通过一个人传递消息的信息。类似地，若 $<u,v> \notin R$ 和 $<u,v> \notin R^{(2)}$，但是有 $s \in A, t \in A$，使 $<u,s> \in R, <s,t> \in R$ 和 $<t,v> \in R$，于是 $<u,v> \in R^{(3)}$。这意味着 u 对 v 即使不能通过少于 2 人传递消息，但是可以通过 2 人中继而传递消息。也就是说，$R^{(3)}$ 包含了所有像 u 到 v 这样的可以通过两个人传递消息的情况…… 如果按此讨论下去，$R^{(i)}$ 包含了所有可以通过 $i-1$ 个人传递消息的信息。定理 3.8 是说，为计算所有任意两人间，从一人到另一人可以直接或通过另外若干人中继而传递消息的信息，在公式（3.51）中只需计算到关系 R 的不超过 n 次幂。

一般如果有 $<u,v> \in R^{(m)}$，且 $m > n$（n 是人群 A 中的人数），即 u 通过 $m-1$ 人将消息传递给 v（$m-1 \geq n$），那么定理 3.8 断言这样的消息链的两端 $<u,v>$ 已经包含于公式（3.51）中，而且这样的消息链上至多只有 n 个结点。事实上，考虑到 A 中共有 n 个人，所以若 u 对于 v（$u \neq v$），不能直接传递消息，但是可以间接联系，则一定可以通过至多 $n-2$ 个人中继实现（这时有 $<u,v> \in R^{(k)}, 2 \leq k \leq n-1$）；再把一个人 u 可以将由他发出的消息反馈回自己的情况也考虑进去（$u = v$），则至多不过是通过其余 $n-1$ 个人中继就能做到（这时有 $<u,v> \in R^{(k)}, 2 \leq k \leq n$）。这就是说，在上述 m（$m \geq n+1$）人中间，必有某人是重复出现的。所以说，任意两个人 u,v（可以包括 $u = v$ 的情况），如果可以通过多于 $n-1$ 个人实现联系的话，那么这个消息链一定包含了某些“消息环”（在消息的传递中，某人两次接受到消息

或两次向别人传递消息——这里是可兼或)。当然这对于从 u 到 v 传递消息来说不是必须的。当我们将所有这些“环”都删除之后，得到的一定是一条结点数不多于 n 的消息链（$u \neq v$）或消息环($u=v$)。最后这一点说明了若 $<u,v>\in R^{(m)}$，且 $m>n$，则必有 $<u,v>\in R^{(k)}$，$1\leq k\leq n$。

上面这段话给出了定理 3.8 的一个实际问题的背景，但确实又给我们提供了严格证明的启发。读者可以由此给出定理的严格证明。

【例 3.17】 设 $A=\{a,b,c,d\}$，$R=\{<a,b>,<b,c>,<c,d>,<d,a>\}$ 和 $S=\{<a,b>,<b,c>,<a,c>,<c,a>\}$。试求 $t(R)$ 和 $t(S)$。

解 首先写出 R 和 S 关系矩阵

$$\boldsymbol{M}_R=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix} \qquad \boldsymbol{M}_S=\begin{bmatrix}0&1&1&0\\0&0&1&0\\1&0&0&0\\0&0&0&0\end{bmatrix}$$

R 的自身的复合关系的关系矩阵是

$$\boldsymbol{M}_{R^{(2)}}=\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix} \qquad \boldsymbol{M}_{R^{(3)}}=\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix}$$

$$\boldsymbol{M}_{R^{(4)}}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \qquad \boldsymbol{M}_{R^{(5)}}=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}=\boldsymbol{M}_R$$

$$\boldsymbol{M}_{R^{(6)}}=\boldsymbol{M}_{R^{(4)}}\circ\boldsymbol{M}_{R^{(2)}}=\boldsymbol{M}_{R^{(2)}},\boldsymbol{M}_{R^{(7)}}=\boldsymbol{M}_{R^{(3)}},\cdots$$

可见，当 $i>4$，$R^{(i)}$ 的矩阵必与 $R,R^{(2)},R^{(3)},R^{(4)}$ 中的某一个相等，所以

$$t(R)=R\cup R^{(2)}\cup\cdots=R\cup R^{(2)}\cup R^{(3)}\cup R^{(4)}$$

$$\boldsymbol{M}_{t(R)}=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}$$

R 的传递闭包是 A 上的一个全域关系。这是预料中的。因为如果画出 R 的关系图看，是一个包含了 A 中一切元素的闭环。

另外对关系 S 有

$$\boldsymbol{M}_{S^{(2)}}=\begin{bmatrix}1&0&1&0\\1&0&0&0\\0&1&1&0\\0&0&0&0\end{bmatrix} \qquad \boldsymbol{M}_{S^{(3)}}=\begin{bmatrix}1&1&1&0\\0&1&1&0\\1&0&1&0\\0&0&0&0\end{bmatrix}$$

$$\boldsymbol{M}_{S^{(4)}}=\begin{bmatrix}1&1&1&0\\1&0&1&0\\1&1&1&0\\0&0&0&0\end{bmatrix} \qquad \boldsymbol{M}_{S^{(5)}}=\begin{bmatrix}1&1&1&0\\1&1&1&0\\1&1&1&0\\0&0&0&0\end{bmatrix}$$

$$\boldsymbol{M}_{S^{(6)}}=\begin{bmatrix}1&1&1&0\\1&1&1&0\\1&1&1&0\\0&0&0&0\end{bmatrix}=\boldsymbol{M}_{S^{(5)}},\boldsymbol{M}_{S^{(7)}}=\boldsymbol{M}_{S^{(6)}}\circ\boldsymbol{M}_{S}=\boldsymbol{M}_{S^{(5)}},\cdots$$

这一次，因为从关系矩阵可见，$S^{(3)}$ 以后的复合关系中已不再出现新的序偶。最后

$$t(S)=S\cup S^{(2)}\cup\cdots=S\cup S^{(2)}\cup S^{(3)}$$

$$\boldsymbol{M}_{t(S)}=\begin{bmatrix}1&1&1&0\\1&1&1&0\\1&1&1&0\\0&0&0&0\end{bmatrix}$$

这个结果是可以预期的，因为结点 d 是弧点。

3.3 等价关系和集合的划分

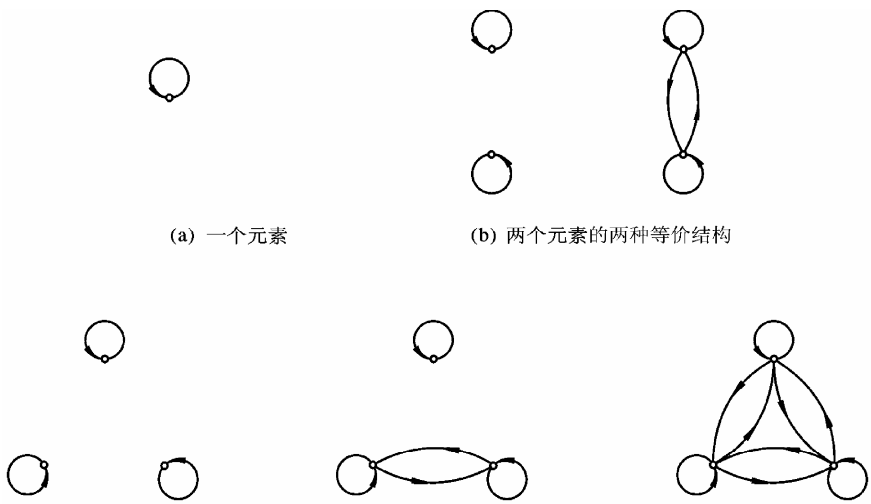
本节的讨论限制在 A 上的二元关系。

3.3.1 等价关系

等价关系是一种经常会遇到的二元关系。

定义 3.28 设 R 是 A 上的二元关系。R 是等价关系，当且仅当 R 是自反的、对称的和可传递的。

图 3.6 给出了含有 1 至 3 个元素的集合上的所有可能的等价关系的关系图结构。



(a) 一个元素　　(b) 两个元素的两种等价结构

(c) 三个元素的三种等价结构

图 3.6　等价关系的关系图

【例 3.18】 整数集 $\mathbf{Z}$ 上的模 k（$k>1$ 的整数）同余关系可定义如下：

$$R=\{<i,j>|i,j\in\mathbf{Z},(\exists q)(q\in\mathbf{Z}\wedge i-j=q\cdot k)\}\tag{3.52}$$

试证 R 是 $\mathbf{Z}$ 上的等价关系。

证明

（1）证明 R 是自反的。任取 $i \in \mathbf{Z}$。因为 $(i-i)=0\cdot k$，所以 R 是自反的，即 $i=i(\mathrm{mod}\,k)$。

（2）证明 R 是对称的。任取 $i,j \in \mathbf{Z}$，并假设 i,j 是模 k 同余的，即有 $(i-j)=q\cdot k$。于是 $(j-i)=(-q)\cdot k$，即 j,i 也是模 k 同余的。

（3）证明 R 是传递的。任取 $i,j,l \in \mathbf{Z}$，并假设 i,j 和 j,l 分别是模 k 同余的，有 $(i-j)=q\cdot k$ 和 $(j-l)=p\cdot k$，于是 $i-l=(i-j)+(j-l)=(q+p)\cdot k$。显然，$(p+q)\in\mathbf{Z}$，所以 i,l 是模 k 同余的。

以下是从一个特殊的例子出发，揭示一个集合 A 上的等价关系 R 与集合 A 的若干特别的子集（这些子集将 A 划分成若干块）之间的关系。

设 A 是某班级学生的集合，定义一个所谓“同姓氏关系” R 于其上：

$$R=\{<s,t>\mid s,t\in A,\ s\text{和}t\text{是同姓氏的}\}$$

容易验证，R 是等价关系。我们总可以将姓氏相同的学生分在一组，姓氏不同的一定在不同组。于是全体学生被分成若干小组，每一组的人数可能不一定相同，但是在同一组中的任何两人（包括每个人与他自己）都是同姓的，即都有上述定义的等价关系，而分别在不同组里的两人一定不具有这种等价关系。在此问题中，每一学生小组叫做一个按“同姓氏关系”诱导（产生）出的**等价类**。很显然，两个不同等价类不相交，所有等价类的并集就是集合 A。

一般情况下，一个有限集 A 上定义的等价关系 R，总可以通过有限次对 A 中元素两两比较而做出它的等价类来。首先，任取一个 $a\in A$，将它放入一空集{}中，产生集合$\{a\}$。其次，在剩下的元素中取 $b\in A-\{a\}$，然后比较 b 和 a，看是否满足 bRa，若是，则将 b 加入到$\{a\}$中去，否则由 b 生成新子集$\{b\}$。以后的每一步，均从尚未放入上述任何子集的元素中任取一个，譬如 $c\in(A-\{a\})-\{b\}$，然后用 c 与已生成的每一子集（如$\{a\}$，$\{b\}$）中的每一元素相比较。这时若 cRa，则置 c 于$\{a\}$中生成$\{a,c\}$。否则，若 cRb，则置 c 于$\{b\}$中生成$\{b,c\}$。若不然，产生一个新的子集$\{c\}$……由于 A 中元素个数是有限的，所以，最终经过有限次上述步骤即可得到由 R 诱导的所有等价类。用记号$[a]_R,[b]_R,\cdots$表示这些等价类，而元素 a,b 等等各称做等价类$[a]_R,[b]_R,\cdots$的**代表元素**。由于同一等价类的诸元素彼此两两等价，所以，一个等价类中的每一个元素都可以作为代表元素。

定义 3.29 设 R 是集合 A 上的等价关系。由元素 $a\in A$ 和一切也属于 A 且与 a 有等价关系 R 的元素共同组成的子集，叫做由 a 生成的等价类，记为 $[a]_R$。即

$$[a]_R=\{x\mid x\in A,xRa,a\in A\} \tag{3.53}$$

【例 3.19】 设 $k=3$，求模 3 同余关系诱导的等价类。

解 容易证明，两个整数 $i,j\in\mathbf{Z}$，如果它们的模 3 余数相等 $i(\mathrm{mod}3)=j(\mathrm{mod}3)$，则 i,j 必定为模 3 同余的，即 $i=j(\mathrm{mod}3)$，就是说满足式（3.52）。

由于模数 $k=3$ 时，模 k 余数只可能是 $r=0,1,2$ 三种。所以，模 3 同余关系有 3 个等价类：

$$[0]_R=\{\cdots,-9,-6,-3,0,3,6,9,\cdots\}$$
$$[1]_R=\{\cdots,-8,-5,-2,1,4,7,10,\cdots\}$$
$$[2]_R=\{\cdots,-7,-4,-1,2,5,8,11,\cdots\}$$

定义 3.30 设 R 是集合 A 上的等价关系。由 R 诱导的一切等价类的集合叫做集合 A 关于 R 的**商集**，记为 A/R。即

$$A/R=\{[x]_R\mid x\in A\} \tag{3.54}$$

要注意的是，若 A 含有 n 个元素，以上定义未必包含 n 个等价类，因为两个等价的代表元素 x_1 和 x_2 生成的等价类是相同的。

定理 3.9 设 R 是 A 上等价关系，$a,b\in A$。$<a,b>\in R$，当且仅当 $[a]_R=[b]_R$。

证明

必要性。设 $<a,b>\in R$，来证 $[a]_R=[b]_R$。任取 $x\in A$，设

$$x\in[a]_R \Leftrightarrow xRa$$

因为由假设 $<a,b>\in R(aRb)$，并且 R 是等价关系，所以

$$xRa,aRb\Rightarrow xRb$$

由式（3.53）可知 $x\in[b]_R$，证得 $[a]_R\subseteq[b]_R$。类似可证 $[b]_R\subseteq[a]_R$，于是 $[a]_R=[b]_R$。

充分性。设 $[a]_R=[b]_R$，来证 aRb。事实上，因为 $a\in[a]_R$，由充分性假设，得 $a\in[b]_R$，所以 aRb （$<a,b>\in R$）。

3.3.2 等价关系与划分

定义 3.31 设 $A_1,A_2,\cdots,A_r$ 是 A 的非空子集。若以下等式成立

$$\bigcup_{i=1}^{r}A_i=A$$

和

$$A_i\bigcap A_j=\varnothing\ (1\leqslant i\leqslant r,1\leqslant j\leqslant r,i\neq j)$$

那么这些子集组成的集合叫做 A 的一个划分，并记做 π_A。即

$$\pi_A=\{A_1,A_2,\cdots,A_r\}$$

并称每一子集 A_i 是一个**划分块**。

回到上面关于一个班级学生之间“同姓氏关系”所诱导的所有等价类，这些等价类的集合就是一个划分。

定理 3.10 设 R 是 A 上的等价关系，A 关于 R 的商集 $A/R=\{A_1,A_2,\cdots,A_r\}$，则等价关系 R 与划分 $\pi_A=\{A_1,A_2,\cdots,A_r\}$ 一一对应。

证明

本定理的含义是一个等价关系 R 对应一个以商集 A/R 做成的划分；反之 A 的任一划分 $\pi_A=\{A_1,A_2,\cdots,A_r\}$ 对应一个等价关系 R。而由 R 诱导的商集 A/R 就是划分 π_A。

首先，设 $A/R=\{A_1,A_2,\cdots,A_r\}$ 是 A 关于 R 的商集，来证它也是 A 的一个划分。

任取 $x'\in A$，以 x' 为代表元素，做成等价类 $[x']_R$。因为 $x'\in[x']_R$，所以 $x'\in\bigcup\limits_{x\in A}[x]_R$，即 $A\subseteq\bigcup\limits_{x\in A}[x]_R$。反之，设 $x'\in\bigcup\limits_{x\in A}[x]_R$，必有 $x'\in[x']_R$。又按等价类定义，$[x']_R\subseteq A$，有 $x'\in A$，所以 $\bigcup\limits_{x\in A}[x]_R\subseteq A$，得 $A=\bigcup\limits_{x\in A}[x]_R$。

另外，可证任意两不同的等价类 $[x]_R\neq[y]_R$ 不相交。即，当 $[x]_R\neq[y]_R$，则 $[x]_R\bigcap[y]_R=\varnothing$。我们用反证法。若不然，设有 $[x]_R\bigcap[y]_R\neq\varnothing$，必有 $c\in[x]_R\bigcap[y]_R$，因为 $c\in[x]_R$，$c\in[y]_R$，故 cRx，cRy，因 R 是等价关系，所以 xRy。按定理 3.9，$[x]_R=[y]_R$。矛盾。

至此已证明商集 A/R 的确是 A 的一个划分。

其次，来证明若 $\pi_A=\{A_1,A_2,\cdots,A_r\}$ 是 A 的一个划分，则必有 A 上的一个等价关系 R，并且商集 A/R 就是 π_A。

构造一个 A 上的关系

$$R=\{<x,y>\mid x,y\in A,(\exists i)(x\in A_i\wedge y\in A_i)\}$$

即 xRy，当且仅当 x 和 y 同属一个划分块。剩下的只要证明 R 是等价关系和 π_A 就是 A/R。

R 是自反的。因为任取 $x \in A$，x 不可能出现在两个不同的划分块，故 xRx。

R 是对称的。因为若 $x, y \in A$，且 x 和 y 在同一划分块 A_i 中，则 y, x 也同在 A_i 中。

R 是传递的。因为任取 $x, y, z \in A$。若 x, y 同属 A_i，y, z 同属 A_j，必有 $A_i = A_j$，即 x, z 同属一划分块。若不然，假设 $A_i \neq A_j$，还因为 $y \in A_i, y \in A_j$，故 $y \in A_i \cap A_j \neq \varnothing$。这与 A_i, A_j 是划分块的假设矛盾。

最后，根据关于 R 的定义和商集的定义直接可知，$\pi_A = A/R$。

定理 3.10 实际给出了一种由 A 的一个划分来构造相应的等价关系的方法。

【例 3.20】 设 $A = \{1,2,3\}$。试求 A 上等价关系 R，使之具有商集 $A/R = \{\{1\},\{2,3\}\}$。

解 分别给出笛卡儿积

$$R_1 = \{1\} \times \{1\} = \{<1,1>\}$$

$$R_2 = \{2,3\} \times \{2,3\} = \{<2,2>, <3,3>, <2,3>, <3,2>\}$$

于是

$$R = R_1 \cup R_2 = \{<1,1>, <2,2>, <3,3>, <2,3>, <3,2>\}$$

该等价关系的关系图有图 3.6（c）中第二种结构。

3.4 序关系和哈斯图

3.4.1 序关系

偏序关系是一种具有某些特殊性质的二元关系。例如，实数上的“小于等于”关系，完全集上子集的包含关系，命题演算中全体公式的主析取范式之间的蕴含关系，整数上的整除关系，等等，都是偏序关系。

定义 3.32 设 R 是集合 A 上二元关系。R 是偏序关系，当且仅当 R 是自反的，反对称的和可传递的。

定义 3.33 设 A 上有偏序关系 $\leqslant$（也可简称为**偏序**），则称序偶 $<A, \leqslant>$ 为**偏序集**或**半序集**。

一般来说，人们在文献中常以记号“$\leqslant$”表示一个偏序关系。这时的记号“$\leqslant$”是广义的，它不一定表示在比较两实数时用到的“小于等于”的含义。但在另一方面，当两个元素 x, y 有偏序关系时，又常记为 $x \leqslant y$（含义如同 xRy 一样），并直接读成：x“小于等于” y。

【例 3.21】 设 $A = \{2,3,6,8,12,16,24,32\}$。$R$ 是整除关系

$$R = \{<x, y> \mid x \in A, y \in A, x \mid y\}$$

试证明 R 是偏序。

证明

因为每一非零整数都可整除自己，所以 R 是自反的。

设 $x, y \in A$，$x \mid y$ 和 $y \mid x$。于是必有整数 q, p，使 $y = q \cdot x$ 和 $x = p \cdot y$。即 $y = q(p \cdot y) = (p \cdot q)y$。因为 $y \neq 0$，所以 $p \cdot q = 1$。但 $(p \cdot q)$ 为整数，故 $p = q = 1$，得 $x = y$。R 是反对称的。

设 $x, y, z \in A, x \mid y, y \mid z$。有整数 q, p，使 $y = q \cdot x$ 和 $z = p \cdot y$，即 $z = p(q \cdot x) = (p \cdot q)x$。因 $p \cdot q$ 为整数，所以 $x \mid z$。

证得 R 是自反的，反对称的和传递的，所以 R 是偏序。

3.4.2 偏序关系的哈斯图

观察例 3.21 中偏序的关系图（图 3.7）后发现，偏序的关系图有明显的层次。可将所有结点分成四层，由“低”至“高”分别为 2 和 3，6 和 8，12 和 16 以及 24 和 32 等。还因为一个偏序图，当它包含较多结点时可能会有很多的边，全部画出来就会使图变得杂乱无章难以看清。**哈斯图**就是省略了偏序图中的某些边之后的一种简图。例如图 3.8 所示。可以省略的边有两类：一类是通过每一结点的自闭合的边。另一类是这样的边：若同时存在两条或两条以上的首尾顺序相连的边 $<u,c_1>,<c_1,c_2>,\cdots,<c_i,c_{i+1}>,\cdots,<c_m,v>$，因为偏序是传递的，所以偏序中必有边 $<u,v>$，而最后这条边 $<u,v>$ 就是可省略的。很明显，我们省略的那些边在偏序关系中都是必然会出现的。换句话说，如果需要，我们可以仅仅凭简化后的哈斯图中留下的边，还原出原来的偏序图。

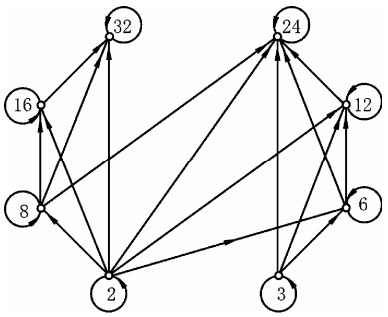


图 3.7　整除关系

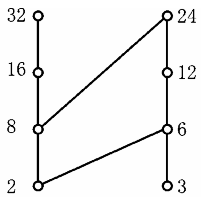


图 3.8　例 3.21 的哈斯图

偏序 $<A,\leqslant>$ 的哈斯图是这样规定的：

1．每一 $x\in A$，用一个小圆圈表示，并且若 $x,y\in A, x\neq y$ 且 $x\leqslant y$，则 y 放在比 x 高的层次上。

2．仅仅画出这样的一些边 $<u,v>$：$u,v\in A,\ u\neq v,u\leqslant v$，但不存在第三个结点 $w\in A,w\neq u,w\neq v$，使得 $u\leqslant w,w\leqslant v$。即可以说仅画出 v **盖住** u 这样的边 $<u,v>$。

3．这样做之后，省略留下的边的箭头号。因为我们可以从结点的层次上知道，哈斯图的边都是指向上方的。

3.4.3 偏序集中的某些特殊元素

在一个偏序 $<A,\leqslant>$ 中，有一些元素有着某些独特的属性。下面就来讨论这些元素。

定义 3.34　设 $<A,\leqslant>$ 是一偏序。集合 $B\subseteq A$。若 B 中任意两元素在 $<A,\leqslant>$ 中都有偏序关系，则称 B 是**链**。

特别当 A 本身是链，称 $<A,\leqslant>$ 是**全序集**。关系“$\leqslant$”称为**全序关系**。

在例 3.21 中，$B_0=\{2\},B_1=\{2,8,16\},B_2=\{2,8,32\},B_3=\{2,8,24\},B_4=\{2,6\},B_5=\{2,12,24\}$ 都是链。

注意：链的定义并不总是像它的名字那样与哈斯图的一条有形的折线相对应，如上面的 B_5 就是一例。

定义 3.35　设 $<A,\leqslant>$ 是偏序，$B\subseteq A$。若存在 $b\in B$，使得一切 B 的元素 $x\in B$ 都满足

$x \leqslant b$，则称 b 是 $<B,\leqslant>$ 的**最大元**，或简称**最大**。

注意：定义中用到了 $<B,\leqslant>$ 这样的符号，因为可以证明，在一个偏序 $<A,\leqslant>$ 中，它的任一非空子集 $B \subseteq A$，如果 B 中的所有结点之间均因袭了它们在 $<A,\leqslant>$ 的偏序关系，则 $<B,\leqslant>$ 仍是偏序集。如果记 B 上偏序关系为 R'，则

$$R' = R \cap (B \times B)$$

（参见本章习题 3.38）或者

$$R' = \{<x,y> \mid x,y \in B, <x,y> \in R\}$$

定义 3.36 设 $<A,\leqslant>$ 是偏序，$B \subseteq A$。若存在 $a \in B$，使得一切 B 的元素 $x \in B$ 都满足 $a \leqslant x$，则称 a 是 $<B,\leqslant>$ 的**最小元**，简称**最小**。

【例 3.22】 设 $A=\{0,1\}$，偏序 $<\rho(A),\subseteq>$。求 $B_0=\{\varnothing\}, B_1=\{\varnothing,\{1\}\}, B_2=\{\varnothing,A\}$，$B_3=\{\{0\},\{1\}\}$ 和 $\rho(A)$ 上的最大元 b_i 和最小元 a_i。

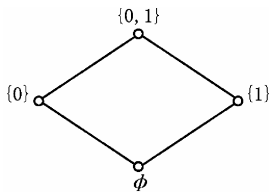


图 3.9　例 3.22 的哈斯图

解　图 3.9 是例 3.22 的哈斯图。

B_0 的最大元和最小元都是 $\varnothing$

B_1 的最大元 $b_1=\{1\}$，最小元 $a_1=\varnothing$

B_2 的最大元是 $b_2=A$，最小元 $a_2=\varnothing$

B_3 没有最大元和最小元

$\rho(A)$ 的最大元是 $b=A$，最小元是 $a=\varnothing$。

定理 3.11　有偏序 $<A,\leqslant>$，$B \subseteq A$。如果 B 有最大（小）元，则最大（小）元是唯一的。

证明

设 b 是 B 的最大元。若还有 $b_1 \in B$ 也是 B 的最大元，则应该有 $b_1 \leqslant b$ 和 $b \leqslant b_1$，于是根据偏序关系的反对称得到 $b_1 = b$。

类似可证最小元如果存在，则是唯一的。

定义 3.37　设 $<A,\leqslant>$ 是偏序，$B \subseteq A$。若有 $d \in B$，使 B 的任何一个元素 $x \in B$，或者有 $x \leqslant d$，或者 x 与 d 是不可比的（即 x 与 d 没有偏序关系，也即 $d \leqslant x$ 或 $x \leqslant d$ 都不成立），则称 d 是 B 的一个**极大元**，简称**极大**。

定义 3.38　设 $<A,\leqslant>$ 是偏序，$B \subseteq A$。若有 $d \in B$，使 B 的任何一个元素 $x \in B$，或者有 $d \leqslant x$，或者 x 与 d 是不可比的，则称 d 是 B 的一个**极小元**，简称**极小**。

显然，最大（小）一定是极大（小），反之不然。

在例 3.22 中，$B_3=\{\{0\},\{1\}\}$，它有两个极大元 $\{0\}$ 和 $\{1\}$，同时它们又都是极小元。

定义 3.39　设 $<A,\leqslant>$ 是偏序，$B \subseteq A$。若有 $s \in A$，使得 B 的任何一个元素 $x \in B$ 都有 $x \leqslant s$，称 s 是 B 的上界。若 s' 是 B 的任一上界，有 $s \leqslant s'$，又称 s 是**上确界**（最小上界），记为 $s = \sup B$。

提醒注意的是，上（下）界可以不属于子集 B。

定义 3.40　设 $<A,\leqslant>$ 是偏序，$B \subseteq A$。若有 $f \in A$，使得 B 的任何一个元素 $x \in B$ 都有 $f \leqslant x$，称 f 是 B 的**下界**。若 f' 是 B 的任一下界，有 $f' \leqslant f$，又称 f 是**下确界**（最大下界），记为 $f = \inf B$。

回到例 3.22 中的 $B_3=\{\{0\},\{1\}\}$，它有上界 $s=\{1\}$ 和下界 $f=\{0\}$，同时也各是 B_3 的上确界和下确界。

但是不要以为一个偏序<$A,\leqslant>$的子集 B 有上界，必有上确界，更不必是有上界必有最大元。下面是一个例子。

【例 3.23】 设 $A=\{a,b,c,d\}$ ，$\leqslant=\{<a,a>,<b,b>,<c,c>,<d,d>,<c,a>,<c,b>,<d,a>,<d,b>\}$ 。

容易验证它是偏序。图 3.10 是它的哈斯图。讨论 $B_1=\{a,b\}$ 和 $B_2=\{c,d\}$ 的最大（小），极大（小），上（下）界和上（下）确界。

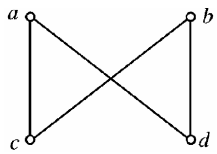


图 3.10　例 3.23 的哈斯图

解

对于 $B_1=\{a,b\}$，它没有最大元，也没有最小元，a,b 都是 B_1 的极大，也是极小。没有上界，有两个下界 c 和 d，但没有下确界。没有上界当然无上确界。

对于 $B_2=\{c,d\}$，它没有最大和最小。c,d 都是极大，也是极小。B_2 有两个上界 a 和 b，但没有上确界。它没有下界和下确界。

定理 3.12　一个偏序集 $<A,\leqslant>$ 的子集 $B\subseteq A$。如果有上（下）确界，则上（下）确界是唯一的。

证明

设 $s\in A$ 是 $<B,\leqslant>$ 的上确界。若 $s'\in A$ 也是一个上确界，按上确界的定义，有 $s'\leqslant s$ 和 $s\leqslant s'$。因为 $<A,\leqslant>$ 是偏序，所以有反对称性，于是 $s'=s$。

类似可证如 $<B,\leqslant>$ 有下确界，可证下确界是唯一的。

要特别说明的是，证明子集的上（下）确界的唯一性的前提是该子集必须有上（下）确界。因为对一个子集而言，可能它并不存在上（下）确界，如例 3.23 的 $\{c,d\}$，它有上界，但无上确界。

3.5　函数及其运算

函数对我们并不是一个陌生的概念。一元函数和多元函数是一种由取自某一集合（称为定义域）的一个或一组元素对应到一个集合的确定元素的规则。例如，一元二次函数 $y=3x^2+x-4$。取定 $x=1$，则 $y=0$；当 $x=-1$ 时，$y=-2$ ……对函数而言，这种从自变量到函数值的对应是唯一的，即一个或一组自变量对应一个且仅仅一个函数值。并且，一般而言，这种唯一性是“单向的”。就是说确定了自变量后，有且只有一个函数值与之对应，而反过来，一个函数值可以对应一个以上的自变量。例如上面提到的一元二次函数 $y=3x^2+x-4$，当 $x=-\frac{1}{3}$ 和 $x=0$ 时，都有 $y=-4$。一般而言函数关系不必是一一对应的。

函数与我们在前一节中讨论的二元关系有密切的联系。事实上，实数集 $\mathbf{R}$ 上的一元函数 $y=3x^2+x-4$，就是一个 $\mathbf{R}$ 上的二元关系，唯一要提到的是上一节讨论的二元关系都是有限的，即构成二元关系的序偶的数目是有限的，而 $y=3x^2+x-4$ 是一个 $\mathbf{R}$ 上的无限个序偶组成的二元关系。它可以按二元关系的描述方式表示成

$$f=\{<x,y>\mid x\in\mathbf{R},y=3x^2+x-4\}$$

但这并不意味着函数与关系没有什么区别。实际上，函数的定义要比关系更严格一些。或者说，函数都是关系，但关系并不一定是函数。即函数是一种附加了一定条件的关系，而

关系是函数的推广。正因为如此，关系普遍具有的性质，函数也有。反之不然。

函数在计算机领域内有很多应用，如开关理论、自动机理论和可计算性理论等。

3.5.1 函数的概念

定义 3.41 设 X 和 Y 是两个非空集合，f 是 X 到 Y 的关系。如果对每一个 $x \in X$，存在唯一的 $y \in Y$，使得 $< x, y > \in f$ 或 (xfy)，则称 f 是 X 到 Y 的函数，记为 $y = f(x)$。

该定义在两个方面限制了一个关系。第一个条件是存在性，即每一个 $x \in X$ 都必须和某个 $y \in Y$ 有关系，也就是 f 的定义域是 X 本身而不可是 X 的真子集。第二个条件是唯一性，即每一个 $x \in X$，只能有一个 $y \in Y$ 与之有关系。这一条件可以表示为：若 $y_1, y_2 \in Y$，且 $y_1 = f(x_1)$ 和 $y_2 = f(x_2)$，且 $x_1 = x_2$，则必有 $y_1 = y_2$。或者描述为：若 $y_1 = f(x_1)$，$y_2 = f(x_2)$，且 $y_1 \neq y_2$，则必有 $x_1 \neq x_2$。

有一些术语，如**变换**、**映像**、**映射**、**运算**等，都是函数的同义词。$f: X \to Y$，或者 $X \xrightarrow{f} Y$ 均可用来表示“f 是 X 到 Y 的函数”。

一个函数 $f: X \to Y$，称 X 是 f 的**定义域**，用 D_f 表示，即 $D_f = X$。

若 $< x, y > \in f$，那么 x 叫**自变量**，y 叫做 x 在 f 下的**函数值**或**像**，或 x 是 y 的**原像**。在讨论函数时，代替 $< x, y > \in f$ 或 xfy 的写法是 $y = f(x)$。将这个符号扩充到整个定义域，就成了 $f(X)$。它表示一个集合，即所有 $x \in X$ 在函数 $f(x)$ 下的像的集合，而非一个函数值，通常称之为函数 f 的**值域**

$$f(X) = \{y \mid y = f(x), x \in X\}$$

值域 $f(X)$ 也可记为 R_f。一般而言，$R_f \subseteq Y$。Y 也叫做**值域包**。

因为函数首先是一个关系。所以表示关系的各种方法在此也都适用。

图 3.11 举了两个 X 到 Y 的关系，但它们都不是函数，其中图 3.11(a)不满足像的存在性，图 3.11(b)不满足像的唯一性。

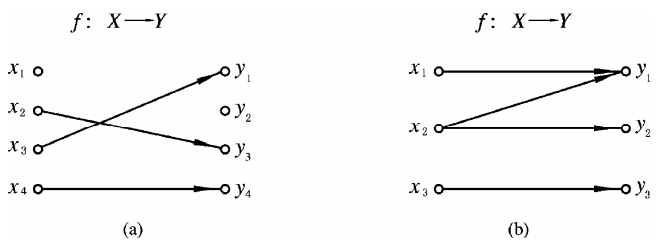


图 3.11 不是函数的关系

而图 3.12 是几个函数的例子。

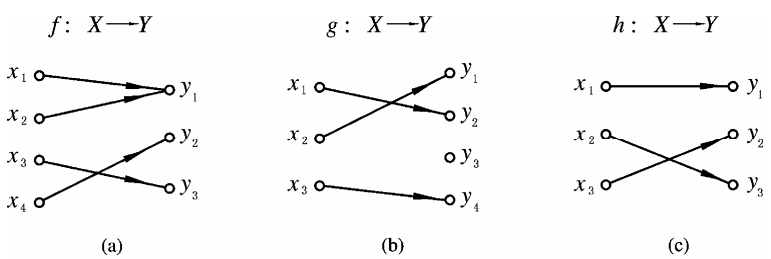


图 3.12　几个函数的例子

特别要比较图 3.11(b)和图 3.12(a)。前者有 $x_2 f y_1$，$x_2 f y_2$，且 $y_1 \neq y_2$，它违背了像的唯一性条件。但后者虽有 $f(x_1)=f(x_2)=y_1$，但它并不违背一个自变量只有一个像的条件。

既然关系可以用矩阵表示，函数当然也行。如图 3.12(a)的函数可用关系矩阵表示为

$$M_f=\begin{bmatrix}1&0&0\\1&0&0\\0&0&1\\0&1&0\end{bmatrix}$$

作为函数的关系矩阵，它必有两个特征：其一是每一行有一个元素为 1，这是和函数像的存在性对应的；其二是每一行仅有一个元素为 1，这是和像的唯一性对应的。

用关系的形式来表示这一函数就是

$$f=\{<x_1,y_1>,<x_2,y_1>,<x_3,y_3>,<x_4,y_2>\}$$

下面再给出一些函数的实例。

（1）$X=\{a,b,1,2\}$，$Y=\{3,5,7\}$，$f=\{<a,7>,<b,5>,<1,3>,<2,5>\}$

显然，$D_f=X$，$R_f=Y$，$f(a)=7$，$f(b)=5$ 等等。

（2）设 $x\in\mathbf{R}$（实数集），

$$f(x)=\begin{cases}x & \text{当}x\geqslant 0\\ -x & \text{当}x<0\end{cases}$$

这里 $D_f=\mathbf{R}$，$R_f\subset\mathbf{R}^+$（非负实数的集合）。

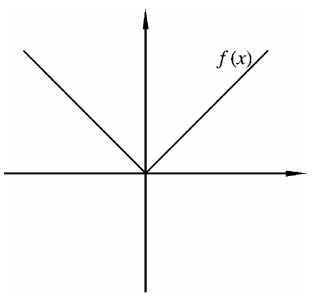


图 3.13　函数的图像

该函数的图像如图 3.13 所示。

（3）设 $(P\wedge Q)\rightarrow R$ 是命题演算的合式公式，其中每一命题变元可以用 V={F,T}中两元素之一代入，其结果可用一真值表描述。所以该合式公式是集合 $V\times V\times V=V^3$ 到 V 的函数。实际上，我们可以把它叫做命题函数。

在这里，我们实际上已经把函数的概念扩充到其定义域是某集合的笛卡尔积的情况，并且把 $V^3\rightarrow V$ 的函数称为集合V上的**三元函数**[*]。

（4）设 E 是完全集。$\rho(E)$ 是它的幂集。对任意两个集合 $A,B\in\rho(E)$，它们的并、交、差运算都是 $\rho(E)\times\rho(E)\rightarrow\rho(E)$ 的函数。而补运算是 $\rho(E)\rightarrow\rho(E)$ 的函数。如上所述，并、交、差都是 $\rho(E)$ 上的二元函数。

（5）设 $\mathbf{N}=\{0,1,2,3,\cdots\}$，$\mathbf{Z}^+=\{1,2,3,\cdots\}$，而 $p=f(z)$ 表示小于等于 z 的正整数中质数的个数。显然 $f(1)=0$，$f(2)=1$，$f(3)=2$，$f(4)=2$ ……且 $p=f(n)$ 是 $\mathbf{Z}^+\rightarrow\mathbf{N}$ 的函数。

这个例子说明了一个问题，即函数并非均可以用**解析表达式**给出。重要的只是从每一自变量对应到唯一一个函数值的规则存在，而这种规则是极为多样化的。

定义 3.42　设 f,g 都是集合 X 到 Y 的函数。若对每一个 $x\in X$，均有 $f(x)=g(x)$，则称 f 和 g 是相等的，记为 $f=g$。即

$$f=g\Leftrightarrow(\forall x)(x\in X\rightarrow f(x)=f(g)) \qquad (3.55)$$

设 $X=\{x_1,x_2,\cdots,x_m\}$ 和 $Y=\{y_1,y_2,\cdots,y_n\}$ 是两个有限集合。$X\times Y$ 共有 $m\times n$ 个序偶。因此，$X\times Y$ 的子集共有 $2^{m\times n}$ 个。每一个这样的子集都是 X 到 Y 的关系，但并非每一个都是函数，

[*] 由此可以定义一个集合 X 上的 n 元函数，就是定义域是笛卡儿积 X^n 的函数。

其中仅有 n^m 个是函数，因为对每一个 $x \in X$ （有 m 个 x ）可以规定任一个 $y \in Y$ （有 n 个）作为 x 的像。故共用 n^m 种不同的方法可以为所有 x 规定它们的像。我们使用符号 Y^X 表示从 X 到 Y 的所有函数的集合就不难理解了。甚至，当 X 或 Y 是无限集时也延用这个符号。

例如， $X=\{a,b\}, Y=\{1,2,3\}$ ，则 $X \times Y$ 有 2×3=6 个序偶， $X \times Y$ 有 2^6 个子集，其中只有 $3^2=9$ 个是函数，它们是

$$f_1=\{<a,1>,<b,1>\},\quad f_2=\{<a,1>,<b,2>\},$$
$$f_3=\{<a,1>,<b,3>\},\quad f_4=\{<a,2>,<b,1>\},$$
$$f_5=\{<a,2>,<b,2>\},\quad f_6=\{<a,2>,<b,3>\},$$
$$f_7=\{<a,3>,<b,1>\},\quad f_8=\{<a,3>,<b,2>\},$$
$$f_9=\{<a,3>,<b,3>\}$$

有一些特别的函数，定义如下。

定义 3.43 设 $f: X \to Y$。如果 $R_f = Y$，也即每一个 $y \in Y$，都是一个（至少一个）$x \in X$ 的像，即

$$(\forall y)(y \in Y \to (\exists x)(x \in X \wedge y = f(x))) \tag{3.56}$$

成立。称函数 f 是 X 到 Y 上的**满映射**，简称**满射**。

我们在本节一开始处曾说过，函数的函数值有存在性和唯一性，并且强调这两个性质是“单向的”。就是说对集合 Y （值域包）而言，并非每一个 $y \in Y$ ，都一定有原像。一定有原像的只是上面定义的满映射。原像的唯一性也类似，有些函数的一个函数值 $y \in Y$ ，可以对应两个不同的原像 $x_1, x_2 \in X$ ，且 $x_1 \neq x_2$（参考图 3.12(a)）。但有一类函数叫入射的，它具有“反向”的唯一性，即一个函数值不会对应两个原像。

定义 3.44 设函数 $f: X \to Y$。如果 $x_1, x_2 \in X$ ，且 $x_1 \neq x_2$ ，就有 $f(x_1) \neq f(x_2)$。即

$$(\forall x_1)(\forall x_2)((x_1 \in X \wedge x_2 \in X \wedge x_1 \neq x_2) \to f(x_1) \neq f(x_2)) \tag{3.57}$$

成立。于是称 f 是 X 到 Y 的**入射**。入射也称为**一对一**的。

函数的定义本身要求对定义域中的每一个元素 $x \in X$ ，它的像是存在的和唯一的。一般地，反过来并不要求对每一个 $y \in Y$ 有原像，也不要求在有原像时，原像是唯一的。但是，对于每一个 $y \in Y$ 必定存在唯一原像的函数，是一种特殊的函数，我们称它为双射。

定义 3.45 设函数 $f: X \to Y$。如果 f 是满射和入射，则称 f 是 X 到 Y 的**双射**。双射也称为一一对应。

图 3.12(b)是入射，但非满射。图 3.12(c)既是满射也是入射，所以图 3.12(c)是双射。从图 3.12 可以分清入射（一对一）与双射（一一对应）的不同之处。

3.5.2 函数的复合

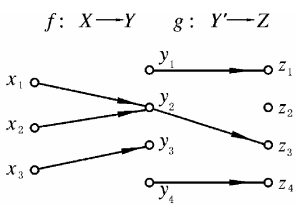


图 3.14 两函数 $f(x), g(x)$ 作为关系的复合 $f \circ g$

类似于二元关系的复合，我们讨论将两个函数做复合的一种运算。

设有两个函数 $f: X \to Y$ 和 $g: Y' \to Z$。按照上一节所述，函数也是关系，因此我们可以按关系一样来做复合关系 $f \circ g$ 。

不难给出图 3.14 中的两函数（按照关系）得出的复合关系，其中 $X=\{x_1,x_2,x_3\}$ ， $Y=\{y_1,y_2,y_3\}$ ， $Y'=\{y_1,y_2,y_4\}$ ， $Z=\{z_1,z_2,z_3,z_4\}$ 。

$$f \circ g = \{< x_1, z_3 >, < x_2, z_3 >\}$$

但这并不是 X 到 Z 的（复合）函数，因为它不满足像的存在性。那么，要使上述两函数 $f(x)$ 和 $g(x)$ 像关系那样复合后仍是一个函数需要什么条件呢？很简单，只要求 f 的值域 R_f 是 g 的定义域 D_g 的子集，即 $R_f \subseteq D_g$。特别是当函数 f 的值域包 Y 就是 g 的定义域的情况。为明确起见，以后在讨论函数的复合时，如不特别声明，就做此假设。

定义 3.46　设有函数 $f: X \to Y$，$g: Y \to Z$，则复合关系 $f \circ g$ 是 X 到 Z 的函数，并称它是 g 与 f 的**左复合**，或 f 和 g 的**复合函数**。按函数的习惯记为 $g \circ f(x)$。即

$$g \circ f = \{< x, z > | x \in X \wedge z \in Z \wedge (\exists y)(y \in Y \wedge y = f(x) \wedge z = f(y))\} \tag{3.58}$$

注意：定义在给定的条件下，断言 f 和 g 的复合关系一定是 X 到 Z 的函数。这是需要证明的。

像的存在性。任取 $x \in X$。因 $f: X \to Y$ 是一函数，所以必有 $y \in Y$，满足 $y = f(x)$。同样因为 $g: Y \to Z$ 是函数，所以有 $z \in Z$，满足 $z = g(y)$。于是 $< x, z > \in g \circ f$（这是按函数习惯表示的复合函数），即 $z = g \circ f(x)$。

像的唯一性。设 $z_1, z_2 \in Z, z_1 \neq z_2$，且有 $x_1, x_2 \in X$，使 $z_1 = g \circ f(x_1), z_2 = g \circ f(x_2)$。来证 $x_1 \neq x_2$。实际上，按复合的定义，存在 $y_1, y_2 \in Y$，使得 $z_1 = g(y_1)$，$z_2 = g(y_2)$ 和 $y_1 = f(x_1)$，$y_2 = f(x_2)$，且因为 g 是 $Y \to Z$ 的函数，f 是 $X \to Y$ 的函数。所以由 $z_1 \neq z_2$ 推知 $y_1 \neq y_2$，进而得出 $x_1 \neq x_2$。

从复合函数的定义直接可得出以下公式

$$g \circ f(x) = g(f(x)) \tag{3.59}$$

图 3.15 是复合函数的一个很直观的例子。

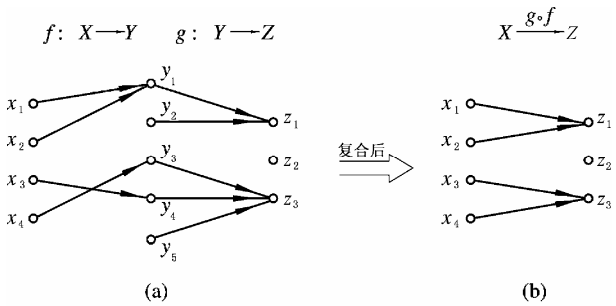


图 3.15　函数复合的图解

【例 3.24】　求图 3.15 给出的 g 与 f 的左复合函数 $g \circ f(x)$。

解

已经说过，任何关系具有的普遍性质，函数也有。现在用关系矩阵的布尔积来计算复合函数（参见本章 3.2.3 小节关系的复合）。

$$M_f = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \qquad M_g = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$M_{g\circ f}=M_f\circ M_g=\begin{bmatrix}1&0&0\\1&0&0\\0&0&1\\0&0&1\end{bmatrix}$$

提醒大家注意的是 $M_{g\circ f}$ 中下标“ $g\circ f$ ”用的是左复合记法。最后复合函数

$$g\circ f=\{<x_1,z_1>,<x_2,z_1>,<x_3,z_3>,<x_4,z_3>\}$$

既然两个函数可复合为一个函数，那么三个适当的函数可以按两种次序依次复合。或者第一、二两个复合后再与第三个复合，或者第一个与第二、三两个复合后的函数再行复合。我们可证明这两种复合的结果是等价的。

设 $f:X\to Y$， $g:Y\to Z$， $h:Z\to W$。则

$$(h\circ g)\circ f=h\circ(g\circ f) \tag{3.60}$$

定理 3.13 函数的复合运算满足结合律。

证明

按式（3.60）给出的函数 $f,g,$ h，有 $X\to Z$ 的复合函数 $g\circ f$ 和 $Y\to W$ 的复合函数 $h\circ g$，都是函数，所以式（3.60）两端仍是两个 $X\to W$ 的函数。至于它们相等，是因为它们作为关系满足关系的结合律（参见式（3.37））。

还有一些有关复合函数的性质。

定理 3.14 设函数 $f:X\to Y,g:Y\to Z$。则

1．若 f,g 都是满射，则 $g\circ f$ 也是满射。

2．若 f,g 都是入射，则 $g\circ f$ 也是入射。

3．若 f,g 都是双射，则 $g\circ f$ 也是双射。

证明

证明其中第 2 条性质，其余留给读者完成。设 f,g 都是入射，任取 $x_1,x_2\in X,$，且 $x_1\neq x_2$，来证 $z_1\neq z_2$，其中 $z_1=g\circ f(x_1),z_2=g\circ f(x_2)$。

事实上，因为 f 是入射，由 $x_1\neq x_2$，得 $y_1\neq y_2$（ $y_1=f(x_1),y_2=f(x_2)$ ）。再因为 g 是入射，所以 $z_1=g(y_1)=g(f(x))=g\circ f(x)$ 和 $z_2=g\circ f(x_2)$ 也不等。

顺便说一下，以上定理中的各命题的逆命题均不是永真的。例如，若 $g\circ f$ 是满射，只能得出 g 是满射； $g\circ f$ 是入射，只能推知 f 是入射等等。

3.5.3 逆函数

一般而言，若 $f:X\to Y$ 是函数，当把它作为关系处理时有逆关系 $f^c:Y\to X$。但由于函数 f 可能不是满射或入射，所以，逆关系 f^c 并不保证原像的存在性和唯一性，一般 f^c 并不是一个函数。很明显，当 f 本身是双射时， f^c 一定也是一个函数。

定义 3.47 设 $f:X\to Y$，如果它的逆关系也是函数，则称它为函数的逆函数，或简称为**逆**，记为 $f^{-1}:Y\to X$。即

$$f^{-1}=\{<y,x>|\ y\in Y\ \wedge\ x\in X\ \wedge\ y=f(x)\}$$

一个函数有逆函数，称此函数是可逆的。

由逆函数的定义可知，若 $y=f(x)$，则 $x=f^{-1}(y)$。

定理 3.15 一个函数可逆的充分必要条件是该函数是双射。

证明

充分性。设 $f:X\to Y$ 是双射，所以也是满射。因此对任一个 $y\in Y$，有 $y=f(x)$（$x\in X$）。又因为 f 是入射，所以对 $y_1,y_2\in Y$，$y_1=y_2$，必有 $x_1,x_2\in X$，满足 $y_1=f(x_1)$ 和 $y_2=f(x_2)$，且 $x_1=x_2$。以上的证明说明对任意 $y\in Y$，它的原像是存在且唯一的。因此 $f:X\to Y$ 可逆。

必要性。又设 f 可逆，来证 f 必是双射。

任取 $y\in Y$，因 f^{-1} 存在，必有 $f^{-1}(y)=x$（$x\in X$）。由逆函数定义可知，$y=f(x)$。故 f 是满射。

另外假设 $x_1,x_2\in X$，$x_1\neq x_2$，于是 $y_1=f(x_1),y_2=f(x_2)$（即 $x_1=f^{-1}(y_1),x_2=f^{-1}(y_2)$），因 f^{-1} 是函数，所以 y_1,y_2 在逆 f^{-1} 下的像是唯一的，即从 $x_1\neq x_2$ 推知 $y_1\neq y_2$，因此 f 是入射。

既然 f 是满射和入射，所以 f 是双射。

由本定理直接可推知，函数的逆存在，则逆函数也是双射。

因为由逆的定义可得

$$(f^{-1})^{-1}=f \tag{3.61}$$

所以 f 是 f^{-1} 的逆函数，因此 f^{-1} 是双射。

最后我们来讨论复合与逆结合的运算。回忆我们说过的一切函数具有关系所具有的最普遍的性质，所以类似公式（3.43）有

$$(g\circ f)^{-1}=f^{-1}\circ g^{-1} \tag{3.62}$$

以上等式成立仅要求 f 和 g 都是可逆的。公式中出现的确实全都是函数。例如 $g\circ f$ 是双射，$(g\circ f)^{-1}$ 是双射，f^{-1},g^{-1} 也都是双射。这不难从 3.5.2 小节和本小节诸定理得到证明。

定义 3.48　集合 X 上的恒等关系 $I_X:X\to X$，称为**恒等函数**。即

$$I_X=\{<x,x>\mid x\in X\}$$

设函数 $f:X\to Y$。易证以下恒等式成立。

$$f\circ I_X=f,I_Y\circ f=f \tag{3.63}$$

定理 3.16　设函数 $f:X\to Y$ 是可逆的。则

$$f^{-1}\circ f=I_X,f\circ f^{-1}=I_Y \tag{3.64}$$

证明

先证明 $f^{-1}\circ f=I_X$。另一式证明可类似给出。首先，f^{-1} 是可左复合 f 的。因为 $f:X\to Y$，$f^{-1}:Y\to X$，并且 $f^{-1}\circ f$ 是 $X\to X$ 的函数。

任取 $x\in X$，按复合函数定义，$f^{-1}\circ f(x)=f^{-1}(f(x))=f^{-1}(y)$，其中 $y=f(x)$。所以，由逆函数定义有 $x=f^{-1}(y)$，即 $f^{-1}\circ f(x)=x$。

习　题

3.1　写出以下各集合的表达式。

（a）所有实系数一元一次方程的解；

（b）直角坐标系中单位圆上的点；

（c）极坐标表示的单位圆及其内的点；

（d）能被 5 整除的数。

3.2 举例说明集合 A,B,C。$A\in B,B\in C$，但 $A\notin C$。

3.3 以下各命题是真还是假？

（a）$\phi\subseteq\phi$；

（b）$\phi\in\phi$；

（c）$\phi\subseteq\{\phi\}$；

（d）$\phi\in\{\phi\}$；

（e）$\{a,b\}\subseteq\{a,b,c,\{a,b,c\}\}$；

（f）$\{a,b\}\in\{a,b,c,\{a,b,c\}\}$；

（g）$\{a,b\}\subseteq\{a,b,\{\{a,b\}\}\}$；

（h）$\{a,b\}\in\{a,b,\{\{a,b\}\}\}$；

（i）$\{a,b\}\in\{a,b,\{a,b\}\}$。

3.4 对任意集合 A,B,C，确定以下各命题是否为真。对真的证明之，若为假，试举一反例。

（a）若$A\in B,B\subseteq C$，则$A\in C$；

（b）若$A\in B,B\subseteq C$，则$A\subseteq C$；

（c）若$A\subseteq B,B\in C$，则$A\in C$；

（d）若$A\subseteq B,B\in C$，则$A\subseteq C$。

3.5 设$A=\{x\mid x<5\wedge x\in\mathbf{N}\},B=\{x\mid x<9\wedge x>0\wedge x$是奇数$\}$。求$A\cap B,A\cup B,A-B,B-A,A\oplus B$。

3.6 若 A,B,C 是任意集合，当 $A\cap B=A\cap C$，并且 $\sim A\cap B=\sim A\cap C$，是否有 $B=C$？试证明之。

3.7 设 A,B 是任意集合。（a）若 $A-B=B$，则 A 与 B 有何关系？（b）若$A-B=B-A$，则 A 与 B 又有何关系？

3.8 求 $\rho(\phi)$ 和 $\rho(\rho(\phi))$及$\rho(\rho(\rho(\phi)))$。

3.9 设 A,B 是任意集合。试证明 $\rho(A)\cap\rho(B)=\rho(A\cap B)$。

3.10 设 $A=\{a,b,c\},B=\{a,c,d,f\}$。试求：

（a）$A\cap B$；

（b）$A\cup B$；

（c）$\{\phi\}\cap A$；

（d）$\phi\cup B$；

（e）$A-B$；

（f）$B-A$，(g)$A\oplus B$。

3.11 设 $A=\{1,2\}$，求 $\rho(A)\times A$和$A\times\rho(A)$。

3.12 A 是一集合，那么 $A\subseteq A\times A$ 可能成立吗？为什么？

3.13 某人拥有的上装的集合是 A，拥有的下装的集合是 B。那么 $A\times B$ 做何解释？

3.14 设 A,B,C,D 是任意集合。求证 $(A\cap B)\times(C\cap D)=(A\times C)\cap(B\times D)$。

3.15 列出从集合 $A=\{a,b,c\}$ 到 $B=\{p\}$ 的所有二元关系。

3.16 在平面直角坐标系中，设 $X=\{x\mid x\in\mathbf{R}\wedge x\geqslant-1\wedge x\leqslant 1\}$，$Y=\{y\mid y\in\mathbf{R}\wedge y\geqslant-1\wedge y\leqslant 1\}$。则 $X\times Y$ 做何几何解释（$\mathbf{R}$ 是实数集）？

3.17 设 $A=\{1,2\},B=\{a,b\}$。求：

（a）$(A\times A)\times B$；

（b）$A\times(A\times B)$。

3.18　设 A,B,C 是任意集合。求证：

（a）$(A\cup B)-C=(A-C)\cup(B-C)$；

（b）$A-(B-C)=(A-B)\cup(A\cap C)$。

3.19　A,B 是任意集合，$\mathbf{E}$ 是完全集。证明：

（a）$(A\cap B)\cup(A\cap\sim B)=A$；

（b）$B\cup\sim((\sim A\cup B)\cap A)=\mathbf{E}$。

3.20　设集合 $A=\{1,2,3,6\}$。其中定义二元关系 L,D 分别是“小于等于”关系和整除关系。若 x 可整除 y，则记为 xDy。用列举法求出 D 和 L，并求 $D\cup L$ 和 $D\cap L$。

3.21　自定义一组关于 $n\times n$ 关系矩阵按对应元素的布尔加法和乘法，然后给出用两个关系的关系矩阵计算其“并”与“交”的公式。

3.22　用列举法写出以下集合 A 上的二元关系，并给出它们的关系图。

（a）$R_1=\{<x,y>|\,0\leqslant x\wedge y\leqslant 3\},A=\{0,1,2,3,4\}$；

（b）$R_2=\{<x,y>|\,2\leqslant x\wedge y\leqslant 7\wedge x\,|\,y\},\ A=\{n\,|\,n\in\mathrm{N}\wedge n\leqslant 10\}$；

（c）$R_3=\{<x,y>|\,0\leqslant x-y<3\},A=\{0,1,2,3,4\}$；

（d）$R_4=\{<x,y>|\,x,y$ 互为质数$\}$，$A=\{2,3,4,5,6\}$。

3.23　设 $A=\{1,2,3,4\}$，$P=\{<1,2>,<2,4>,<3,3>\}$，$Q=\{<1,3>,<2,4>,<4,2>\}$。求 $(P\cap Q),\ (P\cup Q)$，$\mathrm{dom}P$，$\mathrm{dom}Q$，$\mathrm{ran}P$，$\mathrm{ran}Q$，$\mathrm{dom}(P\cap Q)$，$\mathrm{ran}(P\cup Q)$。

3.24　写出题 3.23 中 P,Q 和 $P\cap Q,P\cup Q$ 的关系矩阵，并与用题 3.21 中定义的运算所得结果比较。

3.25　集合 $A=\{1,2,3\}$ 上的下述关系：

$R=\{<1,1>,<1,2>,<1,3>,<3,3>\}$

$S=\{<1,1>,<1,2>,<2,1>,<2,2>,<3,3>\}$

$T=\{<1,1>,<1,2>,<2,2>,<2,3>\}$

$\varnothing$

$A\times A$

分别按自反性、对称性、反对称性和传递性分类。

3.26　举出集合 $A=\{1,2,3\}$ 上关系的例子，使它们分别具有以下性质：（a）既对称又反对称；（b）既不对称又不反对称；（c）传递的。

3.27　证明：若 A 上关系 R 和 S 是自反、对称和传递的，则 $R\cap S$ 也是自反、对称和传递的。

3.28　设 R 是 A 上的具有对称性和传递性的二元关系，而且对任何一个 $x\in A$，都有一个 $y\in A$，使 xRy。试证明 R 是等价关系。

3.29　设 R 是 A 上有自反性和传递性的关系。T 是 A 上的关系，$<x,y>\in T$，当且仅当 $<x,y>\in R$ 和 $<y,x>\in R$。证明 T 是等价关系。

3.30　设 R 是 A 上的二元关系。试证 R 是传递的充分必要条件是 $R\circ R\subseteq R$。

3.31　设 R_1,R_2 是 A 上的关系。说明以下命题是真还是假并证明之。

（a）R_1,R_2 都是自反的，则 $R_1\circ R_2$ 也是自反的；

（b）R_1,R_2 都是对称的，则 $R_1\circ R_2$ 也是对称的；

（c） R_1, R_2 都是传递的，则 $R_1 \circ R_2$ 也是传递的；

（d） R_1, R_2 都是反对称的，则 $R_1 \circ R_2$ 也是反对称的。

3.32　设 $A=\{a,b,c\}$，$R=\{<a,a>,<a,b>,<b,c>,<c,b>\}$。求 R 的自反闭包、对称闭包和传递闭包。

3.33　设 $A=\{1,2,3,4\}$，$R=\{<1,2>,<2,1>,<2,3>,<3,4>\}$。用矩阵运算求 R 的自反闭包、对称闭包和传递闭包。

3.34　设 $A=\{a,b,c,d\}$。问：可有几种不同的 A 的划分？写出每一种划分以及与之对应的等价关系。

3.35　设 R, R' 是 A 上的等价关系，举例说明 $R \cup R'$ 不一定是 A 上的等价关系。

3.36　设 C 是全体实部非零的复数的集合。C 上二元关系 S 定义为：对于 $a,b,c,d \in \mathbf{R}$，$(a+ib)S(c+id)$，当且仅当 $a=c$，并且 $|b|=|d|$。证明 S 是 C 上的等价关系。由此诱导出的等价类做何几何解释？

3.37　设 $A=\{3,5,15\}$，$B=\{1,2,3,6,12\}$，$C=\{3,9,27,54\}$。D 为整除关系。画出每一集合上关系 D 的哈斯图，并说明哪些是全序集。

3.38　设 R 是 A 上的关系，$A' \subseteq A$。现定义 A' 上关系 R' 为：$R' = R \cap (A' \times A')$。以下命题是真是假？

（a） R 在 A 上是传递的，则 R' 在 A' 上也是传递的；

（b） R 是 A 上的偏序，则 R' 在 A' 上是偏序；

（c） R 是 A 上的全序，则 R' 是 A' 上的全序。

3.39　图 3.16 给出了集合 A={1,2,3,4}上的四个偏序关系。画出它们的哈斯图，并指出哪些是全序。

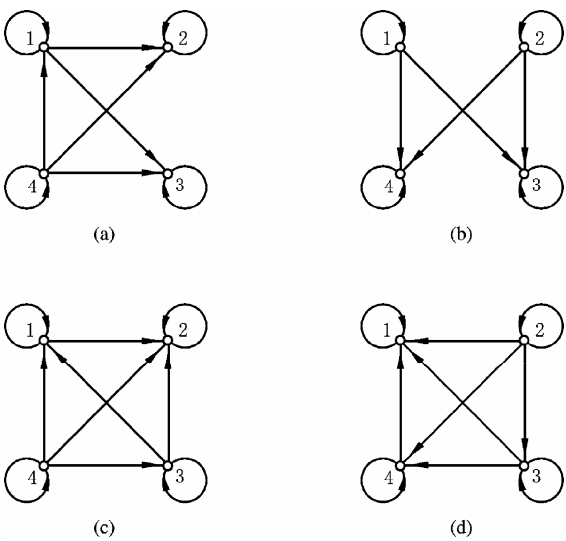


图 3.16　习题 3.39 图

3.40　图 3.17 给出了一个偏序的哈斯图。试绘出它的一般关系图，并写出子集 $\{b,c,d\}$ 上的最大元、最小元、极大、极小、上界、上确界、下界、下确界。

3.41　设 R 是 A 上的二元关系，证明：

（a）若 R 是等价关系，则 R^c 也是等价关系；

（b）若 R 是偏序关系，则 R^c 也是偏序关系；

（c）若 R 是全序关系，则 R^c 也是全序关系。

3.42　$A=\{a,b,c,d\}$，$B=\{1,2,3\}$。试问以下 A 到 B 的关系中，哪些是 A 到 B 的函数？并写出这些函数的定义域 D_f 和值域 R_f。

（a）$f=\{<a,1>,<a,2>,<a,3>\}$；

（b）$f=\{<c,2>,<b,2>,<a,2>\}$；

（c）$f=\{<a,1>,<b,2>,<a,3>\}$。

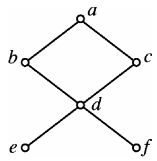


图 3.17　习题 3.40 图

3.43　指出下列函数是满射，或入射，或者双射？

（a）$f:\mathbf{Z}\to\mathbf{Z},\ f(i)=i(\mathrm{mod}3)$；

（b）$f:\mathbf{N}\to\mathbf{N},\ f(i)=\begin{cases}1 & i\text{是奇数}\\ 0 & \text{否则}\end{cases}$；

（c）$f:\mathbf{N}\to\{0,1\},\ f(i)=\begin{cases}1 & i\text{是奇数}\\ 0 & \text{否则}\end{cases}$；

（d）$f:\mathbf{Z}\to\mathbf{N},\ f(i)=|2i|+1$；

（e）$f:\mathbf{R}\to\mathbf{R},\ f(r)=2r-15$。

3.44　设 f,g 是两个函数，$f\subseteq g$ 和 $D_g\subseteq D_f$。证明 $f=g$。

3.45　设 f,g 是两个函数。若 $f\cap g\neq\phi$，试证明 $f\cap g$ 是 $D_{f\cap g}\to R_f\cup R_g$ 上的函数（即 $D_{f\cap g}$ 可能只是 $D_f\cap D_g$ 的某子集）。另外 $f\cup g$ 是否一定为 $D_f\cup D_g\to R_f\cup R_g$ 上的函数？为什么？

3.46　A 和 B 是两个有限集。找出 $f:A\to B$ 是入射的关于 A 和 B 的必要条件。

3.47　$A=\{1,2,3,4\}$。试给出一个 A 上的函数 $f\neq I_A$，且 f 是入射，并求出 $f^{(2)}$，$f^{(3)}$，f^{-1} 和 $f^{-1}\circ f$ 以及 $f\circ f^{-1}$。

3.48　设 $g\circ f$ 是一个复合函数。证明：

（a）若 $g\circ f$ 是满射，则 g 是满射；

（b）若 $g\circ f$ 是入射，则 f 是入射；

（c）若 $g\circ f$ 是双射，则 g 是满射且 f 是入射。

3.49　证明（举一个例子）：若 f 是集合 X 到 Y 的关系，g 是集合 Y 到 Z 的关系，并且，当复合关系 $f\circ g$ 是一个 X 到 Z 的函数时，f 和 g 不必都是函数。

3.50　在集合论的公理化系统中，为避免所谓**罗素悖论**，在用本章 3.1.1 小节中的描述法定义一个集合时，必须保证被定义的集合是一已知集合的子集。例如，定义集合 X

$$X=\{x\mid x\text{是集合，且}x\notin x\}$$

试问 $X\in X$ 或者 $X\notin X$？为什么？

若将集合的描述定义表示为

$$X=\{x\mid x\in A,\text{且}P(x)\}$$

其中 A 为已知集合，P 是任一确定的属性谓词，试说明这样做可以避免罗素悖论。

最后，设 $A=\{a,b\}$，则定义

$$X=\{x\mid x\in\rho(A)\text{，且}x\notin x\}$$

是否悖论？若不是，试用列举法写出集合 X。

第 4 章　数函数和递推关系

在讨论了一般的关系和函数以后，本章将给出一种十分有用的自然数函数，它的定义域是自然数集 **N**={0,1,2,…}，值域包含于实数集 **R**。

4.1　数函数概念

一个**数函数**可以用一个粗体小写字母，如 $\boldsymbol{a}$ 表示。其在自变量为 0,1,2,…,r,…处的函数值则表示为 $a_0, a_1, a_2, \cdots, a_r, \cdots$。

一个数函数可以用穷举法依次列出其函数值，如（$a_0, a_2, \cdots, a_r, \cdots$），若可能，也可用一个 a_r 的**通式**来表达。

【例 4.1】　假设银行存款按每年 3% 的复利计息。若一次存入本金 100 元，则第一年末的本息为 100(1+0.03)，第二年末为 $100(1+0.03)^2$ ……以穷举法写出各年末本息数的数函数为

$$（100, 103, 106.09, \cdots）$$

其中 $\boldsymbol{a}_0$=100 表示存入时刻的值。于是可用通式表为

$$a_r = 100(1+0.03)^r \quad （r \geqslant 0）$$

【例 4.2】　公式

$$a_r = \begin{cases} 0 & 0 \leqslant r \leqslant 3 \\ 0.5(r-3)^2 & r = 4 \\ (r-4)+0.5 & 5 \leqslant r \leqslant 25 \\ (r-25)-0.5(r-25)^2+21.5 & r = 26 \\ 22 & 27 \leqslant r \leqslant 30 \end{cases}$$

表示某一交通工具在 30 分钟之内的每分钟末已行驶的千米数。由此可见，在最初 3 分钟内它处于静止状态，第 4 分钟内加速启动，在随后的 21 分钟内匀速运动，接下来在 1 分钟内减速直至停止，最后持续了 4 分钟静止状态。

4.2　数函数的基本运算

定义 4.1　设 $\boldsymbol{a}$,$\boldsymbol{b}$ 是两个数函数。数函数之和 $\boldsymbol{a}$+$\boldsymbol{b}$ 是一个数函数 $\boldsymbol{c}$，并且

$$c_r = a_r + b_r \quad （r \geqslant 0）$$

定义 4.2　设 $\boldsymbol{a}$,$\boldsymbol{b}$ 是两个数函数。它们的积 $\boldsymbol{a}\,\boldsymbol{b}$ 仍是数函数 $\boldsymbol{d}$，并且

$$d_r = a_r b_r \quad （r \geqslant 0）$$

定义 4.3　设 $\boldsymbol{a}$ 是一数函数，α 是一实数，$\alpha\,\boldsymbol{a}$ 是一数函数 e，并且

$$e_r = \alpha a_r \quad （r \geqslant 0）$$

对于 $\alpha\,\boldsymbol{a}$，也称数函数 $\boldsymbol{a}$ 按 α 的**比例变形**或者**数量积**。

显然，我们可以归纳地定义多个数函数之和、积、数量积。如(**a**+**b**)+**c** 和(**ab**)**c**, α (β **a**)

（其中 α,β 都是实数）等等。

定义 4.4　设 $\boldsymbol{a},\boldsymbol{a}'$是两个数函数。$\boldsymbol{a}=\boldsymbol{a}'$的必要条件是

$$a_r = a'_r \quad (r \geqslant 0)$$

很明显，因为实数的加法和乘法满足交换律和结合律，乘法对加法有结合律，所以按上述方式定义的数函数加法和乘法也满足交换律和结合律。即

1．$\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{b}+\boldsymbol{a}$

2．$\boldsymbol{ab}=\boldsymbol{ba}$

3．$(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}=\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{a})$

4．$(\boldsymbol{ab})\boldsymbol{c}=\boldsymbol{a}(\boldsymbol{bc})$

数量积则满足

5．$\alpha(\beta\boldsymbol{a})=(\alpha\beta)\boldsymbol{a}$

6．$\alpha(\boldsymbol{a}+\boldsymbol{b})=\alpha\boldsymbol{a}+\alpha\boldsymbol{b}$

7．$(\alpha+\beta)\boldsymbol{a}=\alpha\boldsymbol{a}+\beta\boldsymbol{a}$

下面是一些有关数函数之和、之积以及数函数按 α 变形的例子。

设 $\boldsymbol{a},\boldsymbol{b}$ 分别表示家庭中妻子与丈夫的每月收入，则 $\boldsymbol{a}+\boldsymbol{b}$ 就是该家庭的月收入列表。

设$\boldsymbol{a}$表示某国家家庭的平均年消费支出，b表示每年的**恩格尔指数** *，则$\boldsymbol{ab}$表示每年每个家庭平均用于食品的开销。

又设 $\boldsymbol{a}$ 表示上节例 4.1 的数函数，则 $100\boldsymbol{a}$ 则表示存入 10000 元本金后，每一周年末的本金和利息。

卷积是一种很有用的数函数运算。

定义 4.5　设 $\boldsymbol{a},\boldsymbol{b}$ 是两个数函数。卷积 $\boldsymbol{a}*\boldsymbol{b}$ 仍是一数函数 v，并且

$$\begin{aligned} v_r &= \sum_{i=0}^{r} a_i b_{r-i} \\ &= a_0 b_r + a_1 b_{r-1} + \cdots + a_r b_0 \end{aligned}$$

【例 4.3】　设 $\boldsymbol{a}$ 表示开始的一年的年末存入 100 元，即 a_0=100，以后每年末比上一年多存入 10 元的数函数。它给出了每年末的存款数，即

$$a_r = 100(1+0.1r)$$

又设 $\boldsymbol{b}$ 表示开始存入 1 元，以后每年末的本息（设年利率为 3%）。即

$$b_r = (1+0.03)^r$$

于是，第 r 年末总计所得的本息是，第 0 年末存入 100 元的收益 $a_0 b_r$，第一年末存入 110 的收益 $a_1 b_{r-1}$，…，第 r 年存入的本息 $a_r b_0 = a_r = 100(1+0.1r)$ 之和（$b_0 = 1$）：

$$a_0 b_r + a_1 b_{r-1} + \cdots + a_i b_{r-i} + \cdots + a_r b_0$$

因此卷积 $\boldsymbol{a}*\boldsymbol{b}$ 实际表示的是最初存入 100 元，以后每年比上年多存 10 元，在第 r 年末的总本息。

请读者思考一下。若以上假设不变，只是要求第 r 年末的纯利息总和，那么应该怎么做？

---

* 恩格尔指数是经济学家恩格尔提出的用以衡量一个国家人民生活水平的系数，用每年人均用于食品的支出与人均总消费支出之比来表示。

4.3 数函数的母函数

每一个数函数都可以形式上地表示成一个无穷级数，后者称为该数函数的**母函数**。

定义 4.6 设有数函数 $\boldsymbol{a}=(a_0,a_1,\cdots,a_r,\cdots)$，我们称无穷级数

$$a_0+a_1z+a_2z^2+\cdots+a_rz^r+\cdots \tag{4.1}$$

为 $\boldsymbol{a}$ 的母函数，其中 z 是形式变量。

$\boldsymbol{a}$ 的母函数可记为 $\boldsymbol{A}(z)$。

例如数函数$(3^0,3^1,3^2,\cdots,3^r,\cdots)$就可以表示成母函数的形式

$$3^0+3z+3^2z^2+\cdots+3^rz^r+\cdots$$

回忆数学分析中实函数按幂级数展开的方法，上述母函数正是

$$A(z)=\frac{1}{1-3z}$$

的幂级数。

我们可以认为母函数仅仅是数函数的另一种表达形式。因为一个幂级数形式的母函数的系数就是数函数的项；而其形式变量的指数则表明了该项的位置（序号）。更何况一个以幂级数表示的母函数可能被表示成一个简捷的解析式，这将大大方便我们处理某些数函数。

通过直接计算可以证明以下几个定理。

定理 4.1 设 $\boldsymbol{b}=\alpha\,\boldsymbol{a}$，则 $\boldsymbol{B}(z)=\alpha\,\boldsymbol{A}(z)$

例如，数函数

$$b_r=5\times 3^r\ (r\geqslant 0)$$

的母函数就是

$$\boldsymbol{B}(z)=\alpha A(z)=\frac{5}{1-3z}$$

定理 4.2 设数函数 $\boldsymbol{c}=\boldsymbol{a}+\boldsymbol{b}$，它们各自的母函数是 $\boldsymbol{C}(z)$，$\boldsymbol{A}(z)$ 和 $\boldsymbol{B}(z)$，则 $\boldsymbol{C}(z)=\boldsymbol{A}(z)+\boldsymbol{B}(z)$。

例如

$$a_r=2^r+3^r\ (r\geqslant 0)$$

则母函数为

$$\boldsymbol{A}(z)=\frac{1}{1-2z}+\frac{1}{1-3z}$$

再来看一个母函数

$$\boldsymbol{A}(z)=\frac{2+3z-6z^2}{1-2z}$$

它可以改写成

$$\boldsymbol{A}(z)=3z+\frac{2}{1-2z}$$

所以，形式上它表示以下数函数

$$3z+2(2^0+2z+2^2z^2+\cdots+2^rz^r+\cdots)$$

$$=2+7z+2^3z^2+2^4z^3+\cdots+2^{r+1}z^r+\cdots$$

或者写成

$$a_r=\begin{cases}2 & r=0\\ 7 & r=1\\ 2^{r+1} & r\geqslant 2\end{cases}$$

也许现在读者会感到一些惊异：一个看似不能用唯一的规则给出的数函数，竟然被表示成统一的一个母函数！

定理 4.3 设数函数的卷积 $\boldsymbol{c}=\boldsymbol{a}*\boldsymbol{b}$，$\boldsymbol{C}(z)$, $\boldsymbol{A}(z)$, $\boldsymbol{B}(z)$是 $\boldsymbol{c},\boldsymbol{a},\boldsymbol{b}$ 各自的母函数，则 $\boldsymbol{a},\boldsymbol{b}$ 卷积的母函数等于 $\boldsymbol{a},\boldsymbol{b}$ 母函数的积。即是

$$\boldsymbol{C}(z)=\boldsymbol{A}(z)\boldsymbol{B}(z)$$

证明

设 $A(z)=a_0+a_1z+\cdots+a_rz^r$,$B(z)=b_0+b_1z+\cdots+b_rz^r+\cdots$。于是 $A(z)B(z)$的 z^r 系数是

$$a_0b_r+a_1b_{r-1}+\cdots+a_ib_{r-i}+\cdots+a_rb_0$$

而这正是卷积 $\boldsymbol{a}*\boldsymbol{b}$ 的第 r 项的值。

【例 4.4】 数函数 $\boldsymbol{a},\boldsymbol{b}$ 分别定义如下

$$a_r=3^r\ （r\geqslant 0）$$

$$b_r=2^r\ （r\geqslant 0）$$

因为

$$A(z)=\frac{1}{1-3z},B(z)=\frac{1}{1-2z}$$

所以 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的卷积的母函数 $C(z)$是

$$\begin{aligned}\boldsymbol{C}(z)=\boldsymbol{A}(z)\boldsymbol{B}(z)&=\frac{1}{1-3z}\cdot\frac{1}{1-2z}\\ &=\frac{3}{1-3z}-\frac{2}{1-2z}\end{aligned}$$

于是得出卷积

$$c_r=3(3)^r-2(2)^r=3^{r+1}-2^{r+1}$$

下面是求数函数 $\boldsymbol{a}$ 的前 $r+1$ 项和（$\boldsymbol{a}_0+\boldsymbol{a}_1+\cdots+\boldsymbol{a}_r$）的例子。

【例 4.5】 设 $\boldsymbol{a}$ 是数函数，$\boldsymbol{b}$ 是一个常数函数，$b_r=1$（$r\geqslant 0$）。

令 $\boldsymbol{c}=\boldsymbol{a}*\boldsymbol{b}$。显然，

$$c_r=\sum_{i=0}^{r}a_ib_{r-i}=\sum_{i=0}^{r}a_i$$

因为 $\boldsymbol{b}$ 的母函数 $B(z)=\frac{1}{1-z}$，所以

$$C(z)=\frac{1}{1-z}A(z)$$

特别是当 $\boldsymbol{a}$ 也是常数函数 $a_r=1$（$r\geqslant 0$）时，$\boldsymbol{a}*\boldsymbol{b}=\frac{1}{(1-z)^2}$ 就是数函数(1,2,3,⋯,r,⋯)的母函数。

【例 4.6】 求 $1^2+2^2+\cdots+r^2$。

我们先设法求数函数 $(0^2,1^2,2^2,3^2,\cdots,r^2,\cdots)$的母函数 $\boldsymbol{B}(z)$，然后利用上例的结果，从该数函数与恒等数函数 $a_r=1$（$r\geqslant 0$）卷积的母函数 $\frac{1}{1-z}B(z)$得出结果。因为这个母函数的 z^r 的系

数正是$(0^2,1^2,2^2,\cdots,r^2,\cdots)$的前 $r+1$ 项之和。

因为

$$\frac{1}{1-z}=1+z+z^2+\cdots+z^r+\cdots$$

两边微分，有

$$\frac{1}{(1-z)^2}=1+2z+3z^2+\cdots+rz^{r-1}+\cdots$$

由此两边同乘以 z，再度微分，得

$$\frac{\mathrm{d}}{\mathrm{d}z}\frac{z}{(1-z)^2}=1^2+2^2z+3^2z^2+\cdots+r^2z^{r-1}+\cdots$$

两边再同时乘以 z，有

$$z\frac{\mathrm{d}}{\mathrm{d}z}\frac{z}{(1-z)^2}=0^2+1^2z+2^2z^2+3^2z^3+\cdots+r^2z^r+\cdots$$

而

$$z\frac{\mathrm{d}}{\mathrm{d}z}\frac{z}{(1-z)^2}=\frac{z(1+z)}{(1-z)^3}=B(z)$$

就是数函数$(0^2,1^2,2^2,\cdots,r^2,\cdots)$的母函数。因此，

$$\frac{1}{1-z}B(z)=\frac{z(1+z)}{(1-z)^4}$$

的 z^r 项系数 c_r 就是要求的最前 $r+1$ 个自然数平方之和。按照二项式展开定义，$(1-z)^{-4}$ 的 z^r 系数是

$$\begin{aligned}&\frac{(-4)(-4-1)\cdots(-4-r+1)}{r!}(-1)^r\\&=\frac{4\cdot5\cdot6\cdots(r+3)}{r!}(-1)^{2r}\\&=\frac{(r+1)(r+2)(r+3)}{1\cdot2\cdot3}\end{aligned}$$

最终得出 $\frac{z(1+z)}{(1-z)^4}=(z+z^2)\frac{1}{(1-z)^4}$ 中 z^r 的系数是 $(1-z)^{-4}$ 中 z^{r-1} 系数和 z^{r-2} 系数之和

$$c_r=\frac{r(r+1)(r+2)}{1\cdot2\cdot3}+\frac{(r-1)r(r+1)}{1\cdot2\cdot3}=\frac{r(r+1)(2r+1)}{6}$$

按本例开始的分析，即

$$1^2+2^2+\cdots+r^2=\frac{r(r+1)(2r+1)}{6}$$

末尾，我们对二项式展开做一简要的说明。由数学分析可知，函数在点 $x=0$ 上的幂级数展开可表示为

$$f(x)=f(0)+\frac{f'(0)}{1!}x+\frac{f''(0)}{2!}x^2+\cdots+\frac{f^{(r)}(0)}{r!}x^r+\cdots$$

所以

$$(1+x)^n=1+\frac{n}{1!}x+\frac{n(n-1)}{2!}x^2+\cdots+\frac{n(n-1)\cdots(n-r+1)}{r!}x^r+\cdots$$

本例最后计算的 c_r 时，就用到令 $x=-z$，$n=-4$ 后以上展开式中 z^{r-1}和z^{r-2} 的系数。

4.4 递推关系

这一节我们来讨论一种间接地给出一个数函数的方法，这就是递推关系。

一个自然数 r 的阶乘 $r!$可以用通式直接给出：$r!=1\cdot 2\cdot \cdots \cdot r$（$r>0$）；$r!=1$（$r=0$）。

也可以这样定义 r 的阶乘：令 0！=1，并给出公式 $a_r = r\times a_{r-1}$（$r \geqslant 1$）。这样从 $a_0=1$，可以推出 $a_1=1\times 1=1$，从 $a_1=1$，又可推出 $a_2=2\times 1=2\cdots\cdots$ 于是对任意自然数 r，我们总可以通过有限次计算得出 a_r 的值来。

另一个例子是著名的斐波那契（Fibonacci）序列。这个数列的最初两项是 $a_0=1, a_1=1$，而对于 $r\geqslant 2$，有 $a_r = a_{r-1}+a_{r-2}$。即

$$1,1,2,3,5,8,13,21,\cdots$$

一般情况下，想要通过观察法得出 a_r 的一般表达式是困难的。事实上，我们之中大多数人都是通过从该序列连续的两项之和逐渐地得出下一项的方法认识斐波那契数列的。

数函数$(a_0,a_1,\cdots,a_r,\cdots)$，对于任何自然数 $r>r_0$（r_0 是某一确定的自然数），一个联系 a_r 和若干 a_i（$i<r$）的方程叫做**递推关系**。递推关系也被称做**差分方程**。显然，光有一个递推关系，并不能得到数函数本身，还必须事先知道若干点上数函数的值。如已知 a_{r-1}, a_{r-2} 就可以利用递推关系渐次推出所有 a_r 的值。这些事先给定的函数值，叫做**初边条件**。

因此，一个数函数可以用一个递推关系和一组（个）适当给定的初边条件完全地描述。

递推关系是经常使用的一种计算自然数函数的方法。尽管如此，我们仍然有兴趣去研究如何从一个数函数的递推关系和初边条件得到数函数在每一点 r 的值 a_r 的一般表达式（或者它的母函数的解析表达式）。这个过程叫做**解递推关系**。遗憾的是我们并没有一种解递推关系的普遍方法。

本节的重点是如何解所谓**常系数线性递推关系**。

4.4.1 常系数线性递推关系

一个具有下述形式的递推关系叫做常系数线性递推关系

$$C_0a_r + C_1a_{r-1} + \cdots + C_ka_{r-k} = f(r) \qquad (4.2)$$

其中 $C_i(i=0,1,\cdots,k)$ 是常数，$f(r)$是一个定义在自然数上的函数。若 $C_0\neq 0$ 和 $C_k\neq 0$，那么称之为 ***k* 阶常系数递推关系**，也称 ***k* 阶常系数线性差分方程**。

若将式（4.2）等号右边置换为零，即令 $f(r)=0$，得到的是对应的 k 阶线性递推关系的齐次方程

$$C_0a_r + C_1a_{r-1} + \cdots + C_ka_{r-k} = 0$$

例如，斐波那契的递推关系

$$a_r - a_{r-1} - a_{r-2} = 0 \qquad (4.3)$$

是二阶常系数递推关系。

若对自然数 m，数函数 a 的连续 k 个值 $a_{m-k}, a_{m-k+1},\cdots,a_{m-1}$ 为已知，a_m 就可以按式（4.2）计算出来

$$a_m = -\frac{1}{C_0}(C_1a_{m-1} + C_2a_{m-2} + \cdots + C_ka_{m-k} - f(m))$$

进而还可向前求出 a_{m+1}, a_{m+2} 等等。

另外也可向后求出 a_{m-k-1}

$$a_{m-k-1} = -\frac{1}{C_k}(C_0 a_{m-1} + C_1 a_{m-2} + \cdots + C_{k-1} a_{m-k} - f(m-1))$$

下面我们要证明这样的事实，k 阶常系数递推关系（4.2）有 k 个连续的函数值作为初边条件时有唯一解，也即可以唯一确定一个数函数。至于以不连续的 k 个函数值作为初边条件时是否有解，则取决于所给的初边条件的值。以下只就第一类初边条件加以讨论。

方程（4.2）对应的齐次方程的数函数解 $\boldsymbol{a}^{(v)} = (a_0^{(v)}, a_1^{(v)}, \cdots, a_r^{(v)}, \cdots)$ 称为**齐次解**。而满足式（4.2）本身的一个解 $\boldsymbol{a}^{(p)} = (a_0^{(p)}, a_1^{(p)}, \cdots, a_r^{(p)}, \cdots)$ 称为是**特解**。于是 k 阶常系数线性递推关系（4.2）的通解是齐次解和特解之和。

因为

$$C_0 a_r^{(v)} + C_1 a_{r-1}^{(v)} + \cdots + C_k a_{r-k}^{(v)} = 0$$
$$C_0 a_r^{(p)} + C_1 a_{r-1}^{(p)} + \cdots + C_k a_{r-k}^{(p)} = f(r)$$

所以

$$C_0(a_r^{(v)} + a_r^{(p)}) + C_1(a_{r-1}^{(v)} + a_{r-1}^{(p)}) + \cdots + C_k(a_{r-k}^{(v)} + a_{r-k}^{(p)}) = f(r)$$

即，通解 $\boldsymbol{a} = \boldsymbol{a}^{(v)} + \boldsymbol{a}^{(p)}$ 满足递推关系（4.2）。

类似于**常系数线性微分方程**，我们设式（4.2）对应的齐次方程的齐次解是 $A\alpha^r$，稍后会知道实数 α 叫做式（4.2）的特征根（并非是式（4.2）的解）。其中 A 是由初边条件决定的常数。将 $A\alpha^r$ 代入式（4.2）对应的齐次差分方程中（以 $A\alpha^r$ 代替 a_r，$A\alpha^{r-1}$ 代替 a_{r-1} 等等），得

$$C_0 A\alpha^r + C_1 A\alpha^{r-1} + \cdots + C_k A\alpha^{r-k} = 0 \qquad (4.4)$$

化简后成为

$$C_0\alpha^k + C_1\alpha^{k-1} + \cdots + C_{k-1}\alpha + C_k = 0 \qquad (4.5)$$

我们称这个方程为 k 阶常系数线性差分方程（4.2）的**特征方程**，它的根就叫**特征根**。k 阶特征方程（4.4）有 k 个特征根 $\alpha_1, \alpha_2, \cdots, \alpha_k$。

假设所有特征根个个不同（没有重根），不难证明

$$a_r^{(v)} = A_1\alpha_1^r + A_2\alpha_2^r + \cdots + A_k\alpha_k^r \qquad (4.6)$$

也是差分方程（4.2）的齐次解。其中 $A_1, A_2, \cdots, A_k$ 是 k 个由初边条件决定的常数。

当特征方程（4.4）有 m 重根（$1 < m \leqslant k$）α_1 时，可设式（4.6）齐次解中与此 m 重根对应的那 m 项是

$$(A_1 r^{m-1} + A_2 r^{m-2} + \cdots + A_{m-1} r + A_m)\alpha_1^r$$

其中 A_i 决定于初边条件，α_1 是 m 重特征根。和上面讨论一样，$A_m\alpha_1^r$ 是一个齐次解。来证 $A_{m-1} r\alpha_1^r$ 也是一齐次解。为此，对方程（4.4）两边对 r 取导数

$$C_0 r\alpha^{r-1} + C_1(r-1)\alpha^{r-2} + \cdots + C_k(r-k)\alpha^{r-k-1} = 0 \qquad (4.7)$$

因为 α_1 是式（4.4）的 m 重根，由代数理论可知，式（4.4）左边关于 α 的多项式含有 $(r-\alpha_1)^m$ 作为因式，所以特征根 α_1 也一定是导函数方程（4.7）的根（也是 2 至 $m-1$ 次导函数的根）。即

$$C_0 r\alpha_1^{r-1} + C_1(r-1)\alpha_1^{r-2} + \cdots + C_k(r-k)\alpha_1^{r-k-1} = 0$$

两边同乘以 $A_{m-1}\alpha_1$，得

$$C_0A_{m-1}\,r\alpha_1^r + C_1A_{m-1}(r-1)\alpha_1^{r-1} + \cdots + C_kA_{m-1}(r-k)\alpha_1^{r-k} = 0$$

这就是说，当α_1是m重特征根的条件下，$A_{m-1}r\alpha_1^r$确也是齐次解。

类似可证$A_{m-2}r^2\alpha_1^r, A_{m-3}r^3\alpha_1^r, \cdots, A_1r^{m-1}\alpha_1^r$也都是齐次解。

【例 4.7】 试给出斐波那契数列

$$a_r = \begin{cases} 1 & r=0\text{或}r=1 \\ a_{r-1}+a_{r-2} & r>1 \end{cases}$$

的通式。

解

该差分方程$a_r - a_{r-1} - a_{r-2} = 0$的特征方程是

$$a^2 - a - 1 = 0$$

有两个实根是

$$a_1 = \frac{1+\sqrt{5}}{2}, \quad a_2 = \frac{1-\sqrt{5}}{2}$$

显然$a'_r = 0$是满足递推关系$a_r - a_{r-1} - a_{r-2} = 0$的特解，所以斐波那契数列的通解是

$$a_r = A_1\left(\frac{1+\sqrt{5}}{2}\right)^r + A_2\left(\frac{1-\sqrt{5}}{2}\right)^r + 0$$

通过初边条件$a_0 = 1$，$a_1 = 1$可得

$$A_1 + A_2 = 1$$

$$A_1\left(\frac{1+\sqrt{5}}{2}\right) + A_2\left(\frac{1-\sqrt{5}}{2}\right) = 1$$

解这个二元联立方程得

$$A_1 = \frac{5+\sqrt{5}}{10}, \quad A_2 = \frac{5-\sqrt{5}}{10}$$

最终，斐波那契的通解是

$$a_r = \frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^r + \frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^r$$

4.4.2 用母函数求解数函数的通式

下面将讨论另一种求解数函数通式的方法，即通过求解母函数来得到数函数本身。

我们通过一个例子来说明如何从数函数的齐次差分方程求解其母函数的全过程。对于非齐次差分方程的一般讨论已超越本书的范围，有兴趣的读者可以类比对齐次差分方程的处理，自行给出结论。

我们仍以斐波那契数列为例。其差分方程是

$$a_r - a_{r-1} - a_{r-2} = 0 \quad (\text{r}\geqslant 2)$$

为求得其母函数$\boldsymbol{A}(z)$，在上式两边乘以z^r，并从r=2 至r=∞加起来。得

$$\sum_{r=2}^{\infty} a_r z^r - \sum_{r=2}^{\infty} a_{r-1} z^r - \sum_{r=2}^{\infty} a_{r-2} z^r = 0$$

于是

$$(\boldsymbol{A}(z) - a_1 z - a_0) - z(\boldsymbol{A}(z) - a_0) - z^2\boldsymbol{A}(z) = 0$$

注意到 $a_0=1$， $a_1=1$，化简后得

$$A(z)=\frac{1}{1-z-z^2}$$

进一步变形，有

$$\begin{aligned}\boldsymbol{A}(z)&=\frac{1}{\left(1-\frac{1+\sqrt{5}}{2}z\right)\left(1-\frac{1-\sqrt{5}}{2}z\right)}\\&=\frac{H}{1-\frac{1+\sqrt{5}}{2}z}+\frac{K}{1-\frac{1-\sqrt{5}}{2}z}\end{aligned}$$

其中 H,K 为待定常数。将上式通分，继续有

$$\begin{aligned}\boldsymbol{A}(z)&=\frac{1}{1-z-z^2}\\&=\frac{H+K-\frac{1}{2}[H+K-\sqrt{5}(H-K)]z}{\left(1-\frac{1+\sqrt{5}}{2}z\right)\left(1-\frac{1-\sqrt{5}}{2}z\right)}\end{aligned}$$

由于 z 是任意变数，所以有

$$\begin{aligned}H+K&=1\\H+K-\sqrt{5}\,(H-K)&=0\end{aligned}$$

解上述 H,K 的二元联立方程，得

$$H=\frac{5+\sqrt{5}}{10}，\quad K=\frac{5-\sqrt{5}}{10}$$

这样一来，

$$\boldsymbol{A}(z)=\frac{(5+\sqrt{5})/10}{1-\left(\frac{1+\sqrt{5}}{2}\right)z}+\frac{(5-\sqrt{5})/10}{1-\left(\frac{1-\sqrt{5}}{2}\right)z}$$

因为 $A/(1-kz)$ 是数函数 $a_r=Ak^r$ 的母函数，所以斐波那契的通式是

$$a_r=\frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^r+\frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^r$$

这和例 4.7 所得结果是一致的。

习　　题

4.1　一只皮球从 20 米高处落下，每次弹起的高度都是原来落下时高度的一半。

（a） a_r 表示第 r 次弹起的最大高度。写出此数函数 $\boldsymbol{a}$ 的通式。

（b） b_r 表示第 r 次弹起后损失的高度。以 a_r 表示 b_r。

4.2　一化工厂的生产自动线上，用温度传感器（一种将被测环境的温度转变为电信号以便传回控制中心，并由电脑重新转化为温度信息的前端部件）每隔 30s 测量反应釜的温度。记 a_r 为第 r 次测得温度。若开始 300s 内以恒定速率从 100℃上升至 120℃，然后保持这个温

度。写出 a_r 表达式。

4.3 设 $\boldsymbol{a},\boldsymbol{b}$ 是两个数函数。它们分别是

$$a_r = r(\mathrm{mod}17)$$

$$b_r = \begin{cases} 0 & r(\mathrm{mod}3)=0 \\ 1 & \text{否则} \end{cases}$$

（a）设 $c_r = a_r + b_r$。当 r 是什么值时 $c_r = 0$？又当 r 是何值时，$c_r = 1$？

（b）$d_r = a_r b_r$。当 r 是什么值时 $d_r = 0$？当 r 是什么值时 $d_r = 1$？

4.4 给定数函数 $\boldsymbol{a},\boldsymbol{b}$ 的通式如下，求 $\boldsymbol{c}$ 的通式（$\boldsymbol{c}=\boldsymbol{a}*\boldsymbol{b}$）。

（a） $a_r = \begin{cases} 1 & 0 \leqslant r \leqslant 2 \\ 0 & r \geqslant 3 \end{cases}$

$b_r = \begin{cases} 1 & 0 \leqslant r \leqslant 2 \\ 0 & r \geqslant 3 \end{cases}$

（b） $a_r = 1$　一切 r

$$b_r = \begin{cases} 1 & r=1 \\ 2 & r=3 \\ 3 & r=5 \\ -6 & r=7 \\ 0 & \text{其他}r \end{cases}$$

4.5 将以下母函数对应的数函数用一般公式（通式）表示出来。

（a） $\boldsymbol{A}(z) = \dfrac{z^5}{5-6z+z^2}$

（b） $\boldsymbol{B}(z) = \dfrac{1+z^2}{4-4z+z^2}$

（c） $\boldsymbol{C}(z) = \dfrac{1}{(1-z)(1-z^2)(1-z^3)}$

4.6 设有一数函数 $\boldsymbol{a}$ 连续的前几项是

$$1,2,4,7,11,16,22,29,\cdots$$

其中第 0 项 $a_0 = 1$。

（a）用观察法给出 a 的差分方程。

（b）分别用解差分方程和求母函数的方法给出它的一般表达式。

提示：求差分方程的特解时，可设该特解是一个含有合适数目的待定常数的自然数函数，且类型与差分方程中的 $f(r)$ 类同。本题可设特解为一系数待定的 r 的多项式。

第5章　图　　论

本章要讨论关于一般的**图**的概念。这里提及的图虽然和人们通常了解的那些由点和线段组成的几何**图形**有密切的联系，可是在这里，我们将图作为一种描述事物之间复杂关系的数学原型来研究。而图形只是图的一种直观的表示而已。我们说的图当然可以用来解决一些纯粹是图形性质的问题，但更多的时候，人们用图的理论来解决一些看似与图形无直接联系的问题。例如，一个由许多子（小）工程组成的工程决策问题。用图论中的所谓最长路径方法，可以控制诸子工程的工期以保证总工程按期完成或提前完成。在那里，可以很清楚地显示哪些子工程会影响总工期，而哪些则可以有一定的宽限期。

图论在社会科学、语言学、物理、电工和通信工程等很多领域均有它的应用。特别地，图在计算机科学的开关理论和逻辑设计、人工智能、形式语言、信息分析和故障分析等方面起着重要的作用。

和一般的数学理论一样，图的广泛应用取决于它的高度抽象性和理论的缜密性。因此，离散数学中研究的图（不是图形），被建立成一种有严格结构的数学原型。另一方面，在解决任何领域中与图有关的实际问题时，人们可以把它们的问题抽象为一个图的问题，于是有关图的理论就自然成为人们解决这类问题的有力工具了。

尽管在许多时候，我们讨论图的性质而并不依赖图形，尽管在本章一开始就强调了图与图形的不同之处，但考虑到讲述图论的直观性，我们在研究图的时候，仍不时给出相应的图形，甚至有时候也直呼表示某一图的图形为图。

5.1　图的基本概念和术语

图是一种**数学结构**，我们如下给出它的定义。

定义 5.1　图是一个三元组 $G=<V,E,\varphi>$，其中集合 $V=\{v_1,v_2,\cdots,v_n\}$ 称为**点集**，$E=\{e_1,e_2,\cdots,e_m\}$ 称为**边集**，φ 是定义在边集 E 上的函数，其值域系由点集 V 的一些序偶或**无序偶**组成。

序偶已经在第 3 章的笛卡尔积一节中讨论过。无序偶也是由两个属于点集 V 的点 $u,v\in V$ 组成，只是不计这两点的次序。一般用圆括号表示无序偶。如 $(u,v)=(v,u)$。由于一般集合的元素是无次序的，所以无序偶实际上就是一个由两个顶点组成的集合 $\{u,v\}$。不过在图论中，仍习惯用圆括号代替集合的大括号来表示无序偶。

这里是一些最基本的术语。设有图 $G=<V,E,\varphi>$。

顶点或结点：属于集合 V 的每一元素叫做图的顶点或结点。

边：属于集合 E 的元素叫做边。若 $e\in E$，当 $\varphi(e)$ 为有序偶 $<u,v>$ 时，e 叫做**有向边**，并且从起点 u 到终点 v 是这条边的**方向**；当 $\varphi(e)$ 为无序偶 (u,v) 时，e 叫做**无向边**。无向边可以认为是“双向”的。在不致引起混淆的情况下（当 φ 是一个入射时），有时也将边 e 的像（序偶或无序偶）叫做边。对有向边 $<u,v>$，u 称为**起点**，v 称为**终点**；对无向边 (u,v)，两顶点均称为是边的**端点**。

关联：若 $\varphi(e)=<u,v>$（或 (u,v)），则称边 e 关联于点 u 和 v。一回事，也可称点 u 或 v 关联于边 e。并且与同一条无向边 (u,v) 关联的两个顶点 u 和 v 是**相邻的**，而与有向边 $<u,v>$ 关联的两个顶点 u 和 v 就只能说 ***"u 邻接到 v"***，而不是相反。

相邻边：关联于同一结点的两条边是互相相邻的。

有限图：图上点集 V 和边集 E 都是有限集合的时候，称此类图为有限图。本章的讨论限于有限图。

有向图：所有边都是有向边的图。

无向图：所有边都是无向边的图。

混合图：含有有向边和无向边的图。

平行边：若对于 $e_1 \in E$ 和 $e_2 \in E$，当 $\varphi(e_1)=\varphi(e_2)=<u,v>$（或 $=(u,v)$）时，称 e_1 和 e_2 是平行边。

注意：若 $\varphi(e_1)=<u,v>$，而 $\varphi(e_2)=<v,u>$ 时，e_1 与 e_2 并非平行边。从函数角度来考虑，仅当 φ 不是入射时才会出现平行边。

自回路：自回路是一条边，它仅仅关联于图的同一顶点。自回路被看成有向边或无向边是无所谓的。

简单图：不含平行边的有（无）向图叫做简单有（无）向图。

孤点：不与任何边相关联的顶点。

零图：仅含有孤点的图。

多重图：含有平行边的图。

加权图：若图的每一边对应一个非负实数，这样的图叫加权图。该实数叫相应边的边权。加权图可以表示成 $G=<V,E,\varphi,w>$。其中 $w(e)$ 是定义在边集 E 上的权函数，通常 w 的值域是实数的子集。

图 5.1 给出了几个图的图形表示。其中图 5.1（a）和图 5.1（b）含有平行边，都是多重图。图 5.1（c）是简单加权图。另外，图 5.1（a）含有一个自回路和一个孤点。

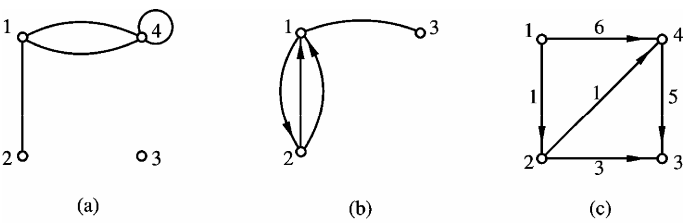


图 5.1　图的图形

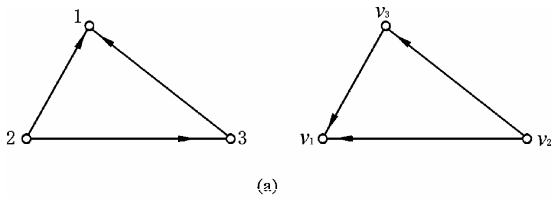
必须指出的是从图的定义可知，用图形表示图时，关联于两点 u,v 的边 $<u,v>$（或 (u,v)）用什么形状的弧段画出是无所谓的。另外，可能有这样的情形：两个看似很不一样的图形，实际表示的是同一个图。或者说，两个图形仅仅是点的名字或形状不同，而作为图来说，它们的结构是一样的。我们把这样的两个图形所表示的两个图叫做**同构的图**。

定义 5.2　设 $G=<V,E>$ 和 $G'=<V',E'>$ 是两个图。若存在一个双射 $h:V \to V'$，此双射保持结点的相邻关系和边的方向。即对 $u,v \in V$，如果 $<u,v> \in E$，当且仅当 $<h(u),h(v)> \in E'$（或 $(h(u),h(v)) \in E'$），那么就称图 G 和 G' 是互相同构的，记为 $G \cong G'$。

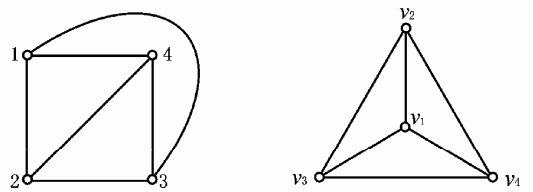
图 5.2（a）中的两个图，只要做出结点之间的如下对应就可证明它们是互相同构的：

$1 \leftrightarrow v_1$　　$2 \leftrightarrow v_2$　　$3 \leftrightarrow v_3$

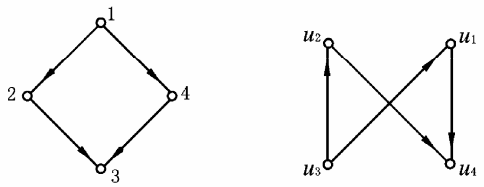
请读者继续完成图 5.2（b）和图 5.2（c）中两两对应的图是互相同构的证明。



(a)



(b)



(c)

图 5.2　同构的图

定义 5.3　在一个有向图中，一个结点 u 的**出度**是指关联于这一点的所有边中的这样一些边的数目，即这些边以 u 为起点。u 的出度记为 $\deg^+(u)$。结点 u 的**入度**是指关联于 u 并以它为终点的边的数目。u 的入度记为 $\deg^-(u)$。而 u 的出度与入度之和叫做 u 的**度**。对有向图有 $\deg(u)=\deg^+(u)+\deg^-(u)$。

无向图的一个顶点 u 的度就是全体与之关联的边数（一个自回路贡献给关联点共 2 度）。

例如，在图 5.1（a）中，$\deg(1)=3$，$\deg(2)=1$，$\deg(3)=0$，$\deg(4)=4$（而不等于 3）。在图 5.1（b）中，$\deg^+(1)=1$，$\deg^-(1)=2$，$\deg(1)=4$（**注意**：图 5.1（b）是混合图）。

定理 5.1　有向图的所有顶点的出度之和等于其所有顶点入度之和。

$$\sum_{v\in V}\deg^+(v)=\sum_{v\in V}\deg^-(v) \tag{5.1}$$

证明是容易的。因为我们可以按边同时统计有向图的出度和入度，而每一边对图的总的出度和入度恰好均贡献 1 度。

定理 5.2　图的总度数等于其总边数的 2 倍。即

$$\sum_{v\in V}\deg(v)=2|E| \tag{5.2}$$

其中 $|E|$ 表示的是边集 E 包含的边数。

只要按边统计图的总度数即可证实式（5.2），因为每一边恰好贡献 2 度给图的总度数。

定理 5.3　任何图中，度数是奇数的结点的数目必定是一偶数。

请读者用式（5.2）完成此定理的证明。

定义 5.4　设G是简单无向图，有n个顶点。当且仅当它的任何两个不同结点间恰有一条边，这样的无向图叫**无向完全图**，并记以K_n。

定义 5.5　设G是简单有向图。若将它的所有边都代之以无向边后，成为一个无向完全图，则G叫做**有向完全图**。

图 5.3 分别给出了$n=5$时的无向完全图和有向完全图之一（按定义，$n\geqslant 3$时，对每一个有n个顶点且不同构的有向完全图不止有一个）。

定理 5.4　一个有n个顶点的完全图共有$n(n-1)/2$条边。

推论　完全图K_n的总度数是$n(n-1)$度。

以上定理和推论都很容易证明，请读者自行完成。

定义 5.6　设$G=<V,E>$是无向图，V含有n个顶点。又设E_k是完全图K_n的边集。则一个由G的点集V和E_k-E为边集的图叫做G的**补图**，记为$\overline{G}=<V,E_k-E>$。

由补图的定义可知，一个图G的补图的补图是G本身，即

$$\overline{\overline{G}}=G \tag{5.3}$$

实际上，$E_k-(E_k-E)=E$。图 5.4 给出了两个互为补图的例子。

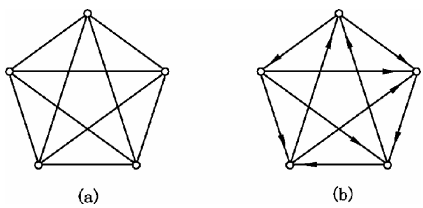


图 5.3　完全图

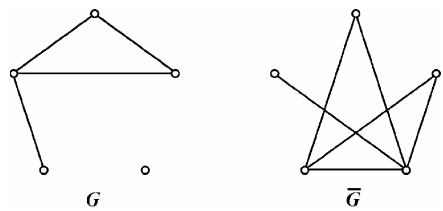


图 5.4　图及其补图

定义 5.7　设有图$G=<V,E>$和$G'=<V',E'>$。若$V'\subseteq V$和$E'\subseteq E$，则称G'是G的**子图**。特别是在$V'=V$而同时有$E'\subseteq E$时，则G'称为是G的**支撑子图**或**生成子图**。

定义 5.8　设$G'=<V',E'>$是$G=<V,E>$的子图。若图$G''=<V'',E''>$中，$E''=E-E'$，且V''中仅仅包含与E''的边关联的顶点，则称G''是G'基于图G的补图。

在图 5.5 中，G'和G''都是G的子图，且G'是G的生成子图，但G''不是。同时G''是G'基于G的补图，G'也是G''基于G的补图。即G'与G''相互为基于G的补图。但相对补图并不总是互补的，这和一般的补图不同。读者可自行举例说明之。

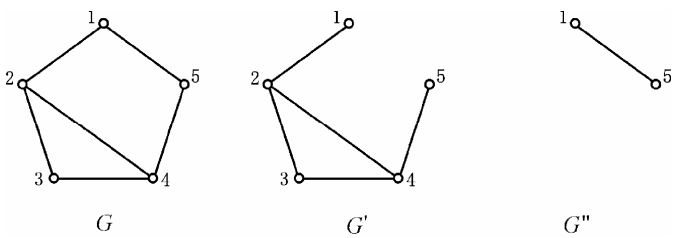


图 5.5　子图与相对补图的例子

5.2　路和回路

本节的讨论先限于有向图，在适当的时候再将结果推广到无向图上去。

在一个图的图形上谈论**路**和**回路**是很直观的。

从图形的某一点 v_{i_1} “出发”，沿着关联于它的某一边所指出的方向（如果有这样的边的话），“到达”另一点 v_{i_2}，再沿着关联于 v_{i_2} 的边所指的方向到达下一点 v_{i_3} ……直至终止于某一点 $v_{i_{k+1}}$。这种由图的顶点开始并结束于顶点的一个由点和边组成的交错序列叫做一条路径，简称为路。

若一条这样的路中至少包含两条不同的边，且起点与终点重合，那么这样一条封闭的路就是回路。自回路通常不包含于回路之列。

定义 5.9 设 $G=<V,E>$ 是一有向图。一个由 G 的点和边组成的交错序列

$$<v_{i_1},e_{j_1},v_{i_2},e_{j_2},\cdots,v_{i_k},e_{j_k},v_{i_{k+1}}> \tag{5.4}$$

叫做 G 的一条**路径**，或者称**路**。

其中任一边 e_{j_i} 均关联于它的相邻两顶点 v_{i_i} 和 $v_{i_{i+1}}$，即 $\varphi(e_{j_i})=<v_{i_i},v_{i_{i+1}}>$。

对于简单有向图，因为 φ 是入射，一条边与唯一的一对点对应。所以简单有向图的路也可以省略式（5.4）中的边，仅用点的序列来表示：

$$<v_{i_1},v_{i_2},\cdots,v_{i_i},\cdots,v_{i_{k+1}}> \tag{5.5}$$

或者

$$<<v_{i_1},v_{i_2}>,<v_{i_2},v_{i_3}>,\cdots,<v_{i_i},v_{i_{i+1}}>,\cdots,<v_{i_k},v_{i_{k+1}}>> \tag{5.6}$$

定义 5.10 一条路中出现的边的次数（重复出现的边计算其重复次数）叫做路的**长度**。

考察图 5.6 所示的有向图。从结点 1 出发而终止于 3 的一些路是：

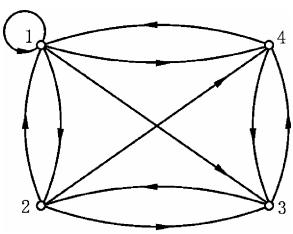


图 5.6 路和回路

$$P_1=<<1,3>>$$
$$P_2=<<1,4>,<4,3>>$$
$$P_3=<<1,2>,<2,3>>$$
$$P_4=<<1,2>,<2,4>,<4,1>,<1,4>,<4,3>>$$
$$P_5=<<1,1>,<1,1>,<1,1>,<1,4>,<4,3>>$$
$$P_6=<<1,2>,<2,1>,<1,1>,<1,2>,<2,3>>$$

以上表示路的序列均采用了简约方式，省略了两相邻边之间的结点。

在讨论路和回路时，我们常常会用到“通过”一词。“通过某一结点”在这里理解为沿着某一边的指向“进入”该结点，然后紧接着又沿着另一边的指向“离开”该结点，或者对起点而言，先离开该结点，而后返回该结点。

定义 5.11 其中所有边均不相同的路叫**简单路**。又若一条路中的所有结点各不相同，则称这样的路为**初等路**。一条初等路必定是简单路，反之不然。

图 5.6 中，P_1,P_2,P_3 是初等路，也是简单路。P_4 是简单路，但不是初等路。

定义 5.12 有向图的起点与终点是同一点的路（显然，至少包含两条以上的边），叫做**有向回路**，其中所有边均不同的叫**简单有向回路**，所有顶点均不同的叫**初等有向回路**。

在图 5.6 中，以下给出的是部分回路。

$$C_1=<<1,2>,<2,1>>$$
$$C_2=<<1,2>,<2,4>,<4,1>>$$
$$C_3=<<1,4>,<4,3>,<3,2>,<2,1>>$$

$$C_4 = <<1,2>,<2,1>,<1,2>,<2,4>,<4,1>>$$

$$C_5 = <<1,4>,<4,1>,<1,2>,<2,4>,<4,1>>$$

以上除C_4和C_5以外均为简单回路，除C_4和C_5以外均为初等回路。

还可以看出，非初等路一定包含有回路，且后者与前者必有公共点。如果公共点多于一次出现于非初等路中，不断地删除这些回路，最终将得到一条初等路。如上述P_4中，删去子回路$<<4,1>,<1,4>>$可得初等路$<<1,2>,<2,4>,<4,3>>$。又若在P_4中删除$<<1,2>,<2,4>,<4,1>>$可得另一初等路$<<1,4>,<4,3>>$。

定义 5.13 设u,v是有向图的两个顶点。如果存在一条从u到v的路，则称顶点u至v是可达的。

约定，图的任一点至它自身总是可达的。

定义 5.14 设u,v是有向图的两个顶点。若u至v是可达的，则u至v的一切路的长度的最小值叫做u至v的**距离**，记为$d<u,v>$。若u至v是不可达的，记$d<u,v>=+\infty$。

约定，$d<u,u>=0$。

要注意的是，即使u与v相互是可达的，也未必有$d<u,v>=d<v,u>$。

关于简单有向图的初等路有以下性质。

定理 5.5 在一个有n个顶点的简单有向图里，任何初等路长度小于等于$n-1$。任何初等回路的长度小于等于n。

证明 因为任何一条初等路的顶点互不相同，而有向图有n个顶点，故初等路至多包含所有n个顶点，它至多含有$n-1$条边，即最长的初等路的长度为$n-1$。

类似可证明定理中有关初等回路的论断。

以下就将上述有向图的种种概念扩充到无向图去。最简单的做法就是在一个无向图中，用一对指向相反的边来代替每一无向边，这样就得到一个有向图。于是上述关于有向图的讨论自然地延伸到了无向图的范畴内。但是，在讨论无向图的回路时，这样的替代要受到一定的限制。这一点，在本章 5.4 节再来说明。还要指出，对无向图而言，任意两点u,v间若有一条路，则称u和v是**连通**的，并且这种连通性是对称的。显然，在无向图中两顶点的距离$d(u,v)=d(v,u)$。

定义 5.15 一个无向图，若其任意两个顶点都是连通的，则称此无向图为**连通图**。

回到有向图继续讨论。

定义 5.16 一个有向图，若忽略它的每一边的指向后成为一无向连通图，则称此有向图是**弱连通**的。

定义 5.17 一个有向图，若它的任意两个顶点之间，至少一个到另一个是可达的，则称此有向图是**单侧连通**的。

定义 5.18 一个有向图，若它的任意一对顶点之间，一个到另一个总是可达的，则称此有向图为**强连通**的。

显然，强连通图一定是单侧连通的。单侧连通图一定是弱连通的。反之均不然。

图 5.7（a）是一单侧连通图G，不是强连通的。图 5.7（b）甚至不是弱连通的。但是图 5.7（a）所示有向图的某些部分（子图）可能是强连通的。例如，取$V'=\{1\}$做成一个零图$G'=<\{1\},\phi>$，按前面的约定，顶点 1 到它自身是可达的，所以它是图 5.7（a）的一个强连通子图。但是否还有一个包含该子图的，而且是G的“更大”的子图也是强连通的呢？在图 5.7（a）中确有一个，

就是$V''=\{1,2,3\}$以及关联于V''中的点的三条边组成的子图G''($G''\supseteq G'$)。再往下讨论，发现图 5.7(a)中不再存在同时是包含G''而自己又是强连通的子图了。像G''这种自身是强连通子图，而又不存在包含它的“更大”的强连通子图，那么，它就叫做强分图。显然，图 5.7（a）中，由各孤点{4}, {5}, {6}独自做成的子图也是“最大”的强连通子图（为什么由{1}或{2}或{3}组成的强连通子图不是“最大”的？），所以它们各自也都是图 5.7（a）的“最大的”强连通子图。

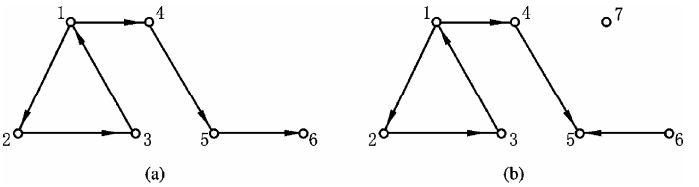


图 5.7　有向图的分图

定义 5.19　一个有向图G，子图$G'\subseteq G$是强连通的，又若有子图$G''\subseteq G$也是强连通的，且如果$G''\supseteq G'$，则必有$G''=G'$，那么G'称为是图G的强连通分图，简称强分图。

类似于强连通分图，我们还可以定义**单侧连通分图**和**弱连通分图**。

讨论图 5.7（b）。它有

强分图：{1,2,3}, {4}, {5}, {6}, {7}

单侧分图：{1,2,3,4,5}, {5, 6}, {7}

弱分图：{1,2,3,4,5,6}, {7}

要说明的是，以上仅以顶点集表示各分图，实际上各分图还包含与此顶点集的每一顶点关联的边。

对于无向图而言，由于其连通性是对称的（总是双向的），所以，对无向图只谈它的连通子图和“最大连通子图”，即**连通分图**。

最后，我们通过一个简单的例子来说明强分图在操作系统检测“资源冲突”中的应用。一个提供多道程序的计算机系统中，每一活动的程序都要占用诸如 CPU、内存、外设、编译程序和数据文件等计算机资源。操作系统则负责分配和管理这些资源，力求不产生资源冲突的情况。若某一程序p_1当前占用了资源r_1，同时又申请资源r_2；另一程序p_2占用着资源r_2，同时又申请资源r_1。当这种情形发生后，若操作系统不曾发现，则系统将处于一种“死锁”状态。这种资源冲突的情形是我们要避免的。有向图可模拟资源分配，发现并纠正死锁状态。

设$P=\{p_1,p_2,\cdots,p_m\}$表示同一段时间内活动的各程序。$R=\{r_1,r_2,\cdots,r_n\}$表示共享资源的集合。每一资源用有向图的结点表示。若某一时刻程序p_i占用r_j并申请r_k，则以一条标记为p_i的边从结点r_j引出并射入r_k。如此画出表示所有程序的边就产生了一个叫做资源分配图的有向图。图 5.8 示例某一时刻的资源配置：

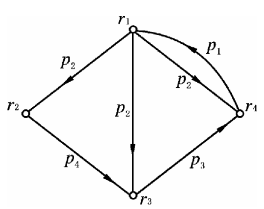


图 5.8　计算机系统的资源分配图

p_1占有r_4，同时申请r_1；

p_2占有r_1，同时申请r_2,r_3,r_4；

p_3占有r_3，同时申请r_4；

p_4占有r_2，同时申请r_3。

显然，当分配图上包含有结点数目大于 1 的强分图时就要发生死锁现象。理论上，纠正死锁的策略就是通过重新分配资源，以使分配图不含强分图的方法。图 5.8 表示一个死锁状态，因它本身是一个强连通

分图。

强分图还可以用来检查一个过程是否是递归的和一个过程通过怎样一些中间过程间接递归的问题。

一种判断强连通图的方法是：如果存在一条包含其所有顶点的有向回路，则一个有向图（或子图）是强连通的。

5.3 图的矩阵表示

我们知道图在现实世界的不同领域有着丰富的应用。换句话说，很多看似不同的问题都可以抽象成图这种数学模型。当一个待解决的问题的规模很大时，相应的图的结点和边的数目将很大。处理规模较大的图往往要依赖计算机去计算。为此必须找到一些便于输入计算机且可以由它运算的表示图的数学模式。矩阵和**链表**是最有效的表达图的工具，并且它们都适合计算机的存取和运算。本节只讨论图的矩阵。其他一些图的存储方式在《数据结构》课程中会有详细的介绍。

回忆在第 3 章我们用矩阵表示一个二元关系。实际上，用图的观点看待一个二元关系，二元关系就是一个图 *。用矩阵代数的运算（加上我们在那里对这种运算的一些扩充）可以方便地解决许多图的问题。

首先介绍有向图的矩阵，然后讨论图的某些特征是如何用矩阵及其运算表达的。

定义 5.20 设 $G=<V,E>$ 是一简单有向图（不含平行边），其中 $V=\{v_1,v_2,\cdots,v_n\}$，并约定了所有关于这些结点的一个次序。$n\times n$ 矩阵 $A(G)=[a_{ij}]$ 称为图 G 的**邻接矩阵**，当且仅当

$$a_{ij}=\begin{cases}1 & \text{如果} <v_i,v_j>\in E\\ 0 & \text{否则}\end{cases}$$

这里对一个图的所有结点约定的次序可以是任意的。对同一个图约定不同的次序显然得到不同的邻接矩阵。但是这些矩阵中的任一个总可以通过适当的行与行和列与列的交换转换成另一个。

从另一角度来说，若有两个 $n\times n$ 邻接矩阵，可以通过行与行和列与列的交换互相转换的话，那么它们所表示的图必是同构的。

从有向图的邻接矩阵 $\boldsymbol{A}(\boldsymbol{G})$可以直接得出图 G 的一些基本特征。例如 $\boldsymbol{A}(\boldsymbol{G})$的第 i 行上值等于 1 的元素的个数等于先前约定的第 i 个结点的出度；而第 j 列元素之和等于所约定第 j 个结点的入度。又若 $a_{ii}=1$，则表示第 i 个结点关联一个自回路。

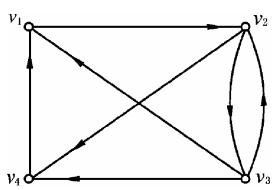


图 5.9 一个有向图

对于图 5.9 给出的有向图，它的邻接矩阵可表示为

$$\boldsymbol{A}(G)=\begin{bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{bmatrix}$$

邻接矩阵的概念经扩充可以表示加权图和多重图。在加权图中，若边权 $w(<v_i,v_j>)=r$，当且仅当 $a_{ij}=r$。对于多重图，若 v_i 相邻到 v_j 的边有 m 条，则 $a_{ij}=m$。

* 一个集合 A 上的二元关系 R，可以写成<$\boldsymbol{A}$, $\boldsymbol{R}$>这样的图。R 中的一个序偶，就是一条边。

要将邻接矩阵扩充至无向图上去，只要将每一无向边看成是一对指向相反的有向边，然后按给出的邻接矩阵定义就可得到无向图的矩阵了。很显然，无向图的邻接矩阵一定是**对称矩阵**。

最后，我们来考察邻接矩阵的幂，看从中给出一些什么信息。

首先 $a_{ij}=1$，表示 v_i 至 v_j 有一条长度为 1 的路。现在以 $a_{ij}^{(r)}$ 表示幂矩阵 A^r 中的第 i 行第 j 列元素。则

$$a_{ij}^{(2)}=\sum_{k=1}^{n}a_{ik}\cdot a_{kj} \tag{5.7}$$

对某一个 k（$1\leqslant k\leqslant n$），$a_{ik}=a_{kj}=1$，这意味着 $<v_i,v_k>$ 和 $<v_k,v_j>$ 都是图的边。若有 s 个这样的 k，意味着图中存在有 s 条从 v_i 可达 v_j 的长度为 2 的路径。从式（5.7）可知，这时 $a_{ij}^{(2)}=s$。类似地我们可知，若 $a_{ij}^{(3)}=t$，就意味着从 v_i 可达 v_j 且有 t 条长度为 3 的路径……因此，以下定理实际已被证实。

定理 5.6 设有向图 $G=<V,E>$ 的邻接矩阵是 A。$a_{ij}^{(r)}$ 表示幂矩阵 A^r 中第 i 行第 j 列元素，则 $a_{ij}^{(r)}$ 的值等于从结点 v_i 至 v_j 长度为 r 的有向路径的数目。

定理的严格证明依赖归纳法。

以图 5.9 中给出的有向图为例。

$$A^2=\begin{bmatrix}0&0&1&1\\2&1&0&1\\1&1&1&1\\0&1&0&0\end{bmatrix}\qquad A^3=\begin{bmatrix}2&1&0&1\\1&2&1&1\\2&2&1&2\\0&0&1&1\end{bmatrix}\qquad A^4=\begin{bmatrix}1&2&1&1\\2&2&2&3\\3&3&2&3\\2&1&0&1\end{bmatrix}$$

由此读者可以验证，因为 $a_{21}^{(2)}=2$，$a_{22}^{(3)}=2$，$a_{42}^{(4)}=1$，所以图 5.9 中存在 2 条长度为 2 的从 v_2 至 v_1 的路，有 2 条长度为 3 的关联于 v_2 的自回路，有 1 条长度为 4 的从 v_4 至 v_2 的路。

由于经常需要了解的只是图中某一点是否可达另一点，并不总是要了解两点之间路径的长度和数量。这样我们就只需去求图的所谓**路径矩阵**。求路径矩阵能简化我们的运算（对计算机来说尤其如此）。

定义 5.21 设 $G=<V,E>$ 是简单有向图，$V=\{v_1,v_2,\cdots,v_n\}$，并约定了一个所有结点的次序。$n\times n$ 矩阵 $P(G)=[p_{ij}]$ 称为是 G 的路径矩阵，当且仅当

$$p_{ij}=\begin{cases}1 & \text{若}v_i\text{至}v_j\text{有一条路}\\0 & \text{否则}\end{cases}$$

我们有两种方法求路径矩阵。先来讨论第一种，用邻接矩阵的幂矩阵来求路径矩阵的方法。做矩阵之和

$$B_r=A+A^2+\cdots+A^r \tag{5.8}$$

用 b_{ij} 表示矩阵和 B_r 的元素，显然 $b_{ij}=a_{ij}+a_{ij}^{(2)}+\cdots+a_{ij}^{(r)}$。所以，$b_{ij}$ 的值表示所有长度小于等于 r 的从 v_i 至 v_j 的路径的数量。若 $b_{ij}>0$，显然相应图的路径矩阵中 $p_{ij}=1$。问题是若 $b_{ij}=0$，只能说明 v_i 至 v_j 没有长度小于等于 r 的路径。那么，为得到 p_{ij} 是否有必要无限制地去增加式（5.8）中 r 的值呢？幸运的是在有限图下不必这样做。如果我们要得到一个有 n 个结点的图的路径矩阵，只要做到 $r=n$ 就可结束了。这个问题我们留给读者去思考（结合考虑

5.2 节的定理 5.5）。

于是，

$$B_n = \sum_{k=1}^{n} A^k = A + A^2 + \cdots + A^n \tag{5.9}$$

B_n 这个矩阵和，已然包含了所有结点之间是否可达的全部信息。若以 b_{ij} 表示它的元素，那么 $b_{ij} > 0$，则 v_i 可达 v_j，否则 v_i 不可达 v_j。即

$$p_{ij} = \begin{cases} 1 & \text{当} b_{ij} > 0 \\ 0 & \text{否则} \end{cases}$$

这就是说，只要对 B_n 的所有元素一一取符号函数

$$sng(b_{ij}) = \begin{cases} 1 & \text{当} b_{ij} > 0 \\ 0 & \text{当} b_{ij} = 0 \\ -1 & \text{当} b_{ij} < 0 \end{cases}$$

就可将 B_n 转换成路径矩阵了（注意，B_n 中的每一元素 $b_{ij} \geqslant 0$）。

$$P(G) = [sng(b_{ij})]$$

其中 b_{ij} 是矩阵和式（5.9）的元素。

求路径矩阵的第二种方法基于邻接矩阵的布尔和与布尔积（参考第 3 章 3.2.3 小节）。

在这里，我们称元素只是 0 或 1 的矩阵为**布尔矩阵**。显然，邻接矩阵与路径矩阵都是布尔矩阵。第 3 章的 3.2.3 小节中，我们已经定义了一个 $\boldsymbol{m \times l}$ 布尔矩阵与另一个 $l \times n$ 布尔矩阵的布尔积以及两个同阶布尔矩阵的布尔和。现在，我们将公式（5.9）中一切普通幂矩阵 A^k 都代之以用布尔积求得的幂矩阵 $\underbrace{A^{(k)} = A \circ A \circ \cdots \circ A}_{k\text{个}}$，并且以布尔和代替式（5.9）中的普通矩阵加法，则可直接求出路径矩阵

$$P = A \oplus A^{(2)} \oplus \cdots \oplus A^{(n)} \tag{5.10}$$

最后我们指出，因为已约定一个结点对自己来说总是可达的。因此，为求出任意两个不同结点之间的可达性，上述式（5.10）中只要累加到 $A^{(n-1)}$ 就行了。因为这样做无非可能是忽略了一条通过所有结点的长度为 n 的初等回路而已。

下面给出了用两种方法求解图 5.9 中图的路径矩阵的方法。

第一种方法。用已在上面求得的各幂矩阵先得出

$$B_4 = A + A^2 + A^3 + A^4 = \begin{bmatrix} 3 & 4 & 2 & 3 \\ 5 & 5 & 4 & 6 \\ 7 & 7 & 4 & 7 \\ 3 & 2 & 1 & 2 \end{bmatrix}$$

于是

$$P = [sng(b_{ij})] = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

第二种方法。先用布尔积求出各幂矩阵

$$A^{(2)}=\begin{bmatrix}0&0&1&1\\1&1&0&1\\1&1&1&1\\0&1&0&0\end{bmatrix}\qquad A^{(3)}=\begin{bmatrix}1&1&0&1\\1&1&1&1\\1&1&1&1\\0&0&1&1\end{bmatrix}\qquad A^{(4)}=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&0&1\end{bmatrix}$$

同样得出路径矩阵

$$P=A\oplus A^{(2)}\oplus A^{(3)}\oplus A^{(4)}=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}$$

由此可知，图 5.9 是一个强连通图。

5.4 树和生成树

5.4.1 无向树的概念

有一种特殊的无向图，叫做**无向树**。

定义 5.22 设 $G=<V,E>$ 是简单无向图。若 G 是连通的，且 G 不含有长度大于 2 的初等回路[*]，则称 G 是无向树。

在图 5.10 中(a),(b)都是无向树，(c),(d)不是无向树。特别是图 5.10(a)，它含有一条长度是 2 的初等路 $<<1,2>,<2,1>>$。这正是我们在定义中没有被排除的唯一一种无向树含有的初等“回路”。

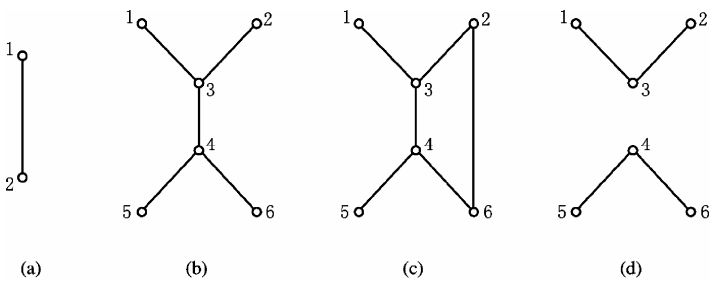


图 5.10 无向图与无向树

可以证明无向树的以下初等性质，而且它们两两互相等价。因此，下面任一初等性质均可以作为无向树的定义。

初等性质：

1．无回路（指长度大于 2 的初等回路，下同），且 $e=v-1$，其中 e 是图的边数，v 是结点数。

2．连通的，且 $e=v-1$。

3．无回路，但添加任意一条关联于不同结点的边之后恰有一个回路。

4．每一对不同的结点间恰有一条初等路。

[*] 因为如不加此限制，一条边可视为长度是 2 的初等回路。所以，这里的讨论将不把无向图转化成有向图。

定义 5.23　如果无向图 G 的生成子图是一棵无向树，称此生成子图为 G 的**生成树**。

定理 5.7　有限的无向连通图 $G=<V,E>$ 必有生成树。

证明　若 G 不含任何回路，则它本身就是生成树。否则，设 C_1 是 G 的一个初等回路。在 C_1 上任意删去一边 $e_1=(u,v)$（参考图 5.11），于是初等回路 C_1 不复存在。剩下的只是证明新产生的子图 $G'=<V,E-\{e_1\}>$ 仍是连通的。若不然，设 G' 不再连通，至少存在两个结点 a,b 不连通，因为 a 与 b 不连通是由于删去了边 (u,v) 引起的，故原图 G 中 a 到 b 间的一条路必定包含 (u,v)。但是结点 u，v 在回路 C_1 上，用 C_1 中删去了边 (u,v) 之后的其余部分 $(u,\cdots,w,\cdots,v)$ 代替该边，仍能构成结点 a,b 之间的路。所以 a,b 不连通是不可能的。若 G' 还含有回路 C_2，用同样的方法可在 C_2 上任意删去一边……由于 G 是有限图，故经过不断删除回路上的边之后，一定可得一无回路的连通子图。这就是图 G 的一个生成树。

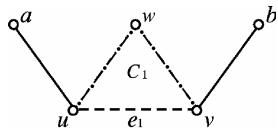


图 5.11　定理 5.7 证明

由于可有多种选择删除回路中的边，一般地说，无向连通图的生成树不是唯一的。但是对同一图 G 而言，为得到它的生成树所需删去边的数目总是固定的。事实上，设 G 有 n 个结点 m 条边，则它的任何生成树一定含有 $n-1$ 条边。所以，必须删除的边数

$$r=m-(n-1)=m-n+1 \qquad (5.11)$$

我们把 r 叫做无向连通图的**秩**。

5.4.2　最小生成树

无向树在很多方面有广泛的应用。下面简单地介绍最小生成树的一个典型应用。

设有 5 个城镇 c_1,c_2,c_3,c_4,c_5。拟用一个最经济的方案铺设公路，以使任意两个城镇均可有公路相连接。为投资尽可能少，两城镇亦可通过第三城镇连通。设图 5.12（a）表示了所有可能铺设的公路的勘测结果，边权是相应公路（用边表示）的建设预算。勘测结果被表示成一个无向连通加权图。现在的问题是如何选择一个最经济的建设方案呢？从数学角度讨论，可以说这是如何求图 5.12（a）的边权之和最小的生成树的问题，或求最小生成树的问题。

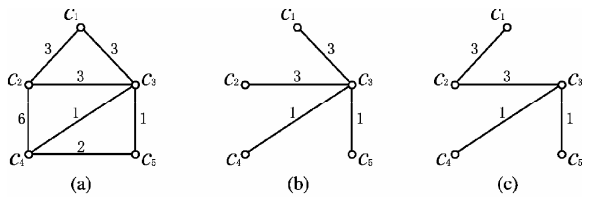


图 5.12　最小生成树问题

定义 5.24　在一个无向连通加权图中，它的所有生成树中边权之和最小的一个叫**最小生成树**。

求解最小生成树的方法有多种。下面介绍其中之一，是**克鲁斯卡**（Kruskal）**方法**。

设无向加权图 $G=<V,E,w>$。$E(T)$ 表示逐步产生且最终成为最小生成树的边集。E' 表示图 G 在计算过程中移去了一些边后所剩的边的集合。初始时，取 $E(T)=\phi$，$E'=E$。假设 G 含有 n 个结点。按生成树的概念，我们就是要进行 $n-1$ 次有效选择，每次在原来图的未被选取的边中挑选一条边权是 E' 中最小的，同时将它添加至已选择的 $E(T)$ 中去，并且不能生成回路。否则就必须从 E' 中舍弃它，并从 E' 中另行选择。直至在 $E(T)$ 中含有 $n-1$ 条边为止。

克鲁斯卡算法：

1．初始化。设置边计数器初值 $i \leftarrow 0, E' \leftarrow E, E(T) \leftarrow \phi$ 。

2．若 $i \geqslant n-1$，则结束。

3．否则，取 $e_0 \in E'$，使得 $w(e_0)=\min\{w(e), e \in E'\}$；$E' \leftarrow E' - \{e_0\}$。

4．判断 e_0 与 $E(T)$中的边是否构成回路，若否，则 $E(T) \leftarrow E(T) \cup \{e_0\}$；$i \leftarrow i+1$。

5．返回第 2 步。

图 5.12 中（b),（c）均为最小生成树，其权值都等于 8（单位的造价）。

5.5 有向树及其应用举例

本节主要讨论有向树中一种有着广泛应用的类型，就是根树。随后举一个应用根树的例子。

5.5.1 有向树的概念

定义 5.25 一个有向图，若不计其边的方向它是一个无向树，这样的有向图叫做**有向树**。图 5.13 给出了有向树的两个例子。

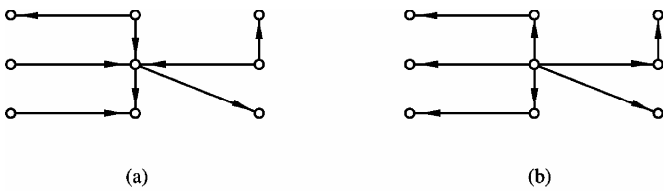


图 5.13 有向树的例子

定义 5.26 一棵有向树，若恰有一个结点入度是 0，其余每一结点入度均为 1，则称此有向树为**根树**。该入度等于 0 的结点叫**树根**，简称**根**。所有出度为 0 的结点叫**树叶**，简称**叶**。出度不为 0 的结点叫**分枝点**。

由于有向树的大部分应用系根树的应用，所以，一般如不事先说明，谈到有向树时就是指根树。图 5.13（b）给出了根树的例子。

约定，一个孤点是一棵有向树，该孤点既是根，又是叶。

以下是根树中的一些术语。

结点的层次：一个结点所在的层次是这样确定的，根处于第 1 层，其余结点所处层次等于根到该结点有向路径的长度加 1。

树的层次：树的层次等于处于最大层次上的叶的层次。树的层次也叫**高度**或**深度**。

如图 5.14（a）中，树的层次是 4。

结点的度：根树一结点的度系指它的出度。

有序树：对于一些应用来说，为同一层次上的所有结点约定一个次序是重要的，这种同层结点有固定次序（如从左至右）的根树叫有序树。

孩子和双亲：根树中两点 u,v，若 u 邻接到 v，则称 v 是 u 的孩子结点，简称孩子。同时 u 是 v 的双亲结点，简称为双亲。

兄弟：若结点 u，v 的双亲是同一个结点，则称它们互为兄弟结点，简称为兄弟。

后裔和祖先：若在根树中结点 u 可达 v，则称 u 是 v 的祖先，而 v 是 u 的后裔。

再来看如图 5.14（a）所示的根树。v_6 的双亲是 v_3，并且它和 v_7，v_8 互为兄弟。v_9 是 v_3 的后裔。

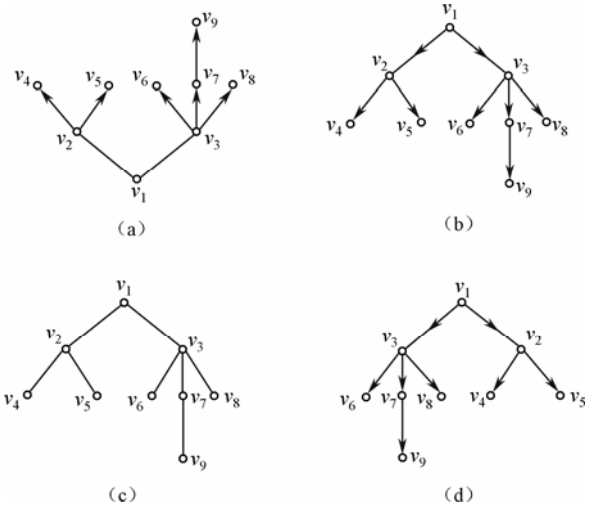


图 5.14　根树及其图示

我们还注意到图 5.14 所示四棵根树是同构的。图 5.14（a）是所谓“自然表示”方法，因为它的根在下，叶子在上。文献中常使用颠倒过来的画法，如图 5.14（b），并且约定同一层次的结点画在一行上，层次愈高的结点愈在下方。这样甚至可以省去每一有向边中的指向箭头（如图 5.14（c））。

还有，对于图 5.14（b）和图 5.14（d）表示的根树，它们是同构的，可以认为是同一根树的不同图示。但是作为有序树而言，它们不是同一棵树。

以后若不特别声明的话，讨论的根树均指有序树。

定义 5.27　结点中最大的度为 m 的根树叫做 m **权树**。

所有叶均在最深一层上，且所有分枝点均为 m 度的根树叫**满 m 权树**。

图 5.15 给出了一棵满二权树。

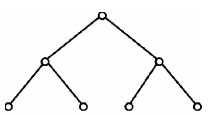


图 5.15　满二权树

根树的结构是递归的。可以删去它的根以及关联于根的所有边，于是得到若干棵更“矮”的**子根树**，它们都以删去的根的孩子为根，它们每一棵都仍然是根树，这样做直至子根树是一叶子为止。

在实际应用中，经常遇到的是所谓**二权树**。为了讨论时的方便，我们约定一个空集是一棵**空二权树**，并且二权树的每一个结点都包含两棵子树，即**左子树**和**右子树**。叶子有两棵空二权树，其他分枝点的两棵子树中可以有一棵是空子树，但是必须明确它是左空子树或者右空子树。也就是说，如果某结点只有一棵子树，那么我们认为该子树是放在左边作为左子树或者放在右边作为右子树是不一样的。像这样必须明确一棵子树的位置的根树一般叫做**位置树**。二权树一般都作为位置树来考虑。

如图 5.16 中所示，给出了最简单的四种非空二权树的结构。其中图 5.16（a）有两棵空子树，图 5.16（b）有非空左子树和空右子树，图 5.16（c）正好与之相反，而图 5.16（d）的两棵子树皆为非空的。特别是图 5.16（b）和图 5.16（c），它们作为有序树是无区别的，即可以将它的唯一一棵非空子树画在其根的左下方、右下方或正下方。但是将图 5.16（b）和图 5.16

（c）看成二权树时，它们就是不同的两棵二权树。图 5.17 也给出了两棵不同的位置树。

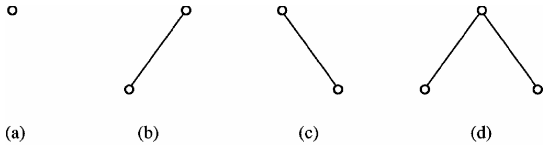


图 5.16　二权树的子树

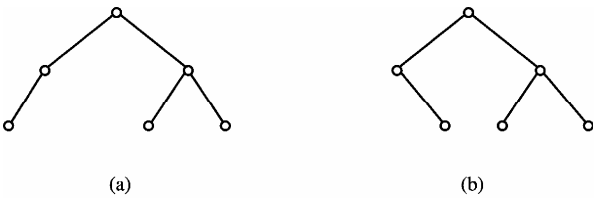


图 5.17　位置树

定义 5.28　有向图 $F=\{T_1,T_2,T_3,\cdots,T_n\}$ 是一个**森林**，当且仅当它的每一弱分图 $T_i(i=1,2,\cdots,n)$ 均为一有序树。若为这些树约定了一个次序，则称此森林为**有序森林**。

图 5.18 给出了一个包含三棵有序树的有序森林。

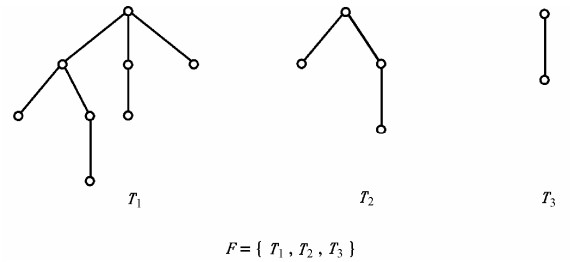


图 5.18　有序森林

5.5.2　根树的一个应用举例

二权树的一个应用是**前缀码**。

客观世界的信息千差万别，为了存储、处理和传递这些信息，必须建立一种能确切地表达信息的方法，于是就产生了所谓**编码**。编码就是将信息用一组代码表示的过程。例如汉字有各种编码，如拼音码、表形码、五笔字形码、国标码等等。英文字母和常用符号等可以用 ASCII（American Standard Code for Information Interchange，即美国标准信息交换码）表示。尽管有各种各样的编码，但是适合计算机应用的所有代码，在最底层的硬件层最终都以符号 0 和 1 组成的串存在。在此意义下，我们可以说计算机编码实际上就是一个完备的字符和各种符号组成的集合与某一由 0 和 1 组成的串的集合之间建立的一个双射。

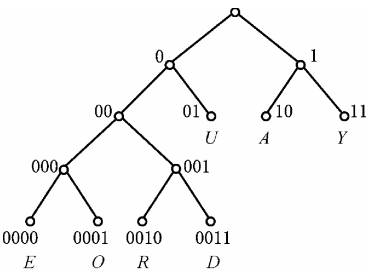


图 5.19　用二权树编制前缀码

有一种很特殊的编码，就是前缀码。我们用图 5.19 来说明如何用二权树产生前缀码。

首先令根的左孩子的编码为 0，右孩子为 1。其余每一结点以它的双亲编码为前缀，然后在此前缀后添加 0

或 1。究竟加 0 还是 1 取决于该结点是其双亲的左孩子或右孩子。最后，我们收集所有叶子的编码组成一个前缀码的集。有趣的是从继承上层结点的代码以作为前缀这一点来说，前缀码的名字是很贴切的。但是，必须特别留意，因为从二权树的结构来看，任何一片叶子均不可能以其他叶子为祖先，所以，如果将一片叶子的前缀码任意一分为二，其中左边一部分代码均不可能是另一片别的叶子的代码。从这种意义上来说，前缀码恰恰又不是“前缀”的。前缀码的这一重要性质，使我们可以很容易从连续写出的一串代码（两代码间无任何间隔符号，如空格符等）中将每一个前缀码分离出来。例如图 5.19，我们为字符集 $\{A,O,U,E,Y,R,D\}$ 安排好它们的编码，如表 5.1 所示。

表 5.1　一组前缀码

A	*O*	*U*	*E*	*Y*	*R*	*D*
10	0001	01	0000	11	0010	0011

对于代码串“100010000011000101001000000100011111”，从生成此前缀码的二权树（图 5.19）的根开始，扫描上述代码串的每一位，当前位是 0 时，沿二权树进入其左子树的根，当前位是 1 时则进入右子树的根。这样每当我们到达一片叶子时，本次扫描到的串就一定是一个完整的代码。再次回到根，并继续扫描代码串中的其余各位，直至代码串的最后一位为止。例如上述代码串最后被析出以下的代码序列：

10 | 0010 | 0000 | 11 | 0001 | 01 | 0010 | 0000 | 10 | 0011 | 11

对照表 5.1 的编码表，不难翻译出这个代码串发送的一条消息是“*ARE　YOU　READY*”。

5.6　欧拉图与哈密顿图

图论的发展史中，有两个非常著名的问题，从而引出了欧拉图与哈密顿图。

5.6.1　欧拉图

欧拉（Leonnard　Euler）是著名的瑞士数学家，1936 年发表了一篇堪称为图论第一篇论文的《哥尼斯堡七桥问题》。问题的由头是这样的，流经哥尼斯堡的普雷格尔河上有两个小岛，小岛和两岸由七座桥梁相互连接（如图 5.20（a））。当时哥市市民中流行着一种健身游戏。有人提出，是否可以从城市的任何地方出发，经过所有七座桥而又不重复通过每一座桥，最后返回出发地呢？后来，欧拉回答了这个问题。他的回答是“不存在这样的巡游路线”。

欧拉将城市的两岸和小岛抽象成四个点，而连接它们之间的桥梁看成是关联于这些点的七条边（图 5.20（b））。于是七桥问题就转化成在图 5.20（b）中寻找一条通过所有边的简单回路的问题。欧拉最后以定理的方式给出了一个图具有通过所有边的简单回路的充要条件。这就是欧拉定理。

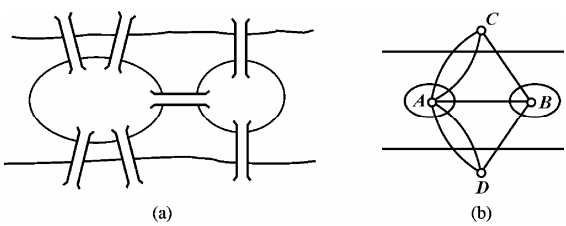


图 5.20　哥尼斯堡七桥问题

显然，我们有理由在以下讨论中排除含有孤点的图。

定义 5.29　在给定的有向图或无向图中，若存在一条包含所有边的简单路，称此路为欧拉路。若存在一条包含所有边的简单回路，则称之为**欧拉回路**。含有欧拉回路的图叫做欧拉图。

定理 5.8　无向图 G 有欧拉路，当且仅当它是连通的，且不存在奇数度结点或者恰有两个奇数度结点。这就是著名的欧拉定理。

推论　无向图是欧拉图，充要条件是它的所有结点的度数都是偶数。

证明　必要性。

设 G 具有欧拉路，要证明 G 是连通图，且或者没有度是奇数的结点，或者恰有两个奇数度结点。

因为 G 有欧拉路，所以它有一条通过所有边的路，由于 G 不含孤点，所以 G 的每一结点至少关联一条边，也即每一结点都在上述那条通过所有边的路上，所以 G 是连通图。

此外，对欧拉路的每一个结点，若它不是起点和终点，那么欧拉路可以多次通过它，进入随即离开，但每通过一次，意味“用去”该结点 2 度，若 m 次经过它，它就有 $2m$ 度。对于起点或终点，若它们是同一个结点，则情形与其余结点一样，必定是偶数度的；否则，对起点而言，当开始遍历欧拉路时，第一次离开它时，“用去”了 1 度，即使以后又 n 次经过它，说明起点是 $2n+1$ 度的。对于另一终点，类似讨论，可知它也必是奇数度的。

充分性。

设图 G 是连通的且无奇数点或恰有两个奇数度点。我们可以据此构造出一条欧拉路。

假设 G 恰有两奇数度结点 u 和 v。因 G 是连通的，所以可以从任一奇数度结点出发，譬如从 u 出发经过一条边到达另一结点。若后者不是结点 v，一定可以从此结点经过一条先前未曾通过的边到达下一个结点（简单路中可多次通过一个结点），只要当前到达的结点不是 v，就可以类似地做下去。因为 G 是连通的有限图，所以经过若干全不相同的边之后，一定可以到达另一奇数度结点 v。将这样一条从 u 到 v 的简单路记为 L_0。如果 L_0 已经包含 G 的一切边，则 L_0 就是欧拉路。否则，删去 L_0 得 G 的子图 G'，G' 至少包含一点 v_1 同时在 L_0 上（G 是连通图）。如果 $v_1 \neq v$，它是偶数度的。如果 $v_1 = v$，它是奇数度的。无论如何，由假设可知，在图 G 中删除了 L_0 后，所余下的子图 G' 的所有结点都必是偶数度的。从 v_1 出发，通过类似以上的讨论可知，必有一条经过 v_1 的简单回路 C_1。若 $L_0 \cup C_1$ 包含了 G 的一切边，则结束，否则再删除 C_1 得到子图 G''，它的所有结点仍都是偶数度的，并且含有通过某一点 v_2 的简单回路 C_2，且 v_2 也在 L_0 上或在 C_1 上。再次删去 C_2。重复上述论述，直至 G 的全部边均包含在 $L_0 \cup C_1 \cup C_2 \cup \cdots \cup C_r$ 中。这就是我们要构造的欧拉路。

以上定理容易推广到有向图的情况。

定理 5.9　设 G 是有向图。G 有一条欧拉路，当且仅当 G 是单侧连通的 *，且每一结点的入度等于其出度或者恰有两点例外，其中一个的出度比入度大 1 度，另一个结点的入度比出度大 1 度。

推论　有向图 G 有一欧拉回路，当且仅当 G 是强连通的，且它的每一结点的出度均等于入度。

---

* 这里，作为定理的充分条件可以用强连通来代替，可是不能用强连通作为定理的必要条件。

这个定理的证明思路基本与上一个定理一样，只要从出度比入度大 1 度的结点出发构造欧拉路即可。不再赘述。

由于我们的证明并不需要假设图无自回路和无平行边，所以欧拉定理对所有图都是正确的。

现在可知，七桥问题为什么是无解的了。

5.6.2 欧拉定理的一个应用举例

这是一个看似与图论无关的问题。机械式二进制码发生器，也称模数鼓。图 5.21 是模数鼓的结构示意图。一个电气接地的金属轮轴上套有一个鼓轮。鼓轮被等分成 16 块，每一块或者是金属制成（图中无细斜线复盖部分），或者是绝缘体做成（有细斜线复盖部分）。有 4 只电刷紧压在鼓轮连续 4 块的表面上，并分别通过电阻 R 汇接至电源 E 的正极上。电源负极电气接地。鼓轮可妥善地定位在沿圆周的 16 等分的每一位置上。显然，若每一电刷与鼓轮的金属块接触，则相应电刷输出为低电位（0），若电刷与绝缘体接触，则输出为高电位（1）。问题是如何排列这些嵌块，可以使鼓轮在 16 个不同位置上输出 16 个各不相同的 4 位二进制码。

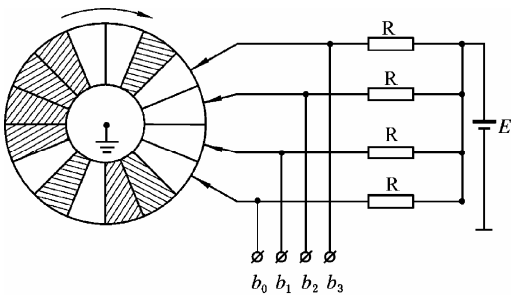


图 5.21　模数鼓轮

分析以上问题可知，若电刷某一位置上输出的是 $b_0\ b_1\ b_2\ b_3$，当鼓轮顺时针（当然也可逆时针）方向转到下一个位置上时，只有两种可能的输出：$b_1\ b_2\ b_3 0$ 或 $b_1\ b_2\ b_3 1$。即上一位置输出的低 3 位等于本次输出的高 3 位。另外，上一位置的值只可能是 $0 b_1\ b_2\ b_3$ 或 $1 b_1\ b_2\ b_3$。我们设法构造一个有向图，用来完全描述鼓轮的这种机理。以一有向边表示一组 4 位二进制码，而关联于同一点的有 4 条边。这 4 条边就是如上面分析时提到的那样，其中射入该结点的两条边的低 3 位相同是 b_1, b_2, b_3，另外射出该结点两边的高 3 位也等于 b_1, b_2, b_3，并以这 3 位来标识该结点。如图 5.22（a）所示。现在的问题是，若可以构造出这样的有向图，它有八个结点和 16 条边，并且像以上所分析的那样让每一结点关联 4 条边，那么根据定理 5.9，的确存在欧拉回路，它通过每一边恰好一次。这意味着鼓轮的设计是可行的。

图 5.22（b）给出了这样的一个有向图。其中一条欧拉回路是 0000,0001,0010,0100,1001,0011,0111,1111,1110,1101,1010,0101,1011,0110,1100,1000。于是，我们将以上序列的最高位依次排列出来是 0000 1001 1110 1011。相应地，鼓轮上嵌块的排列如图 5.21 所示 *。

* 这里，模数鼓的解不是唯一的。

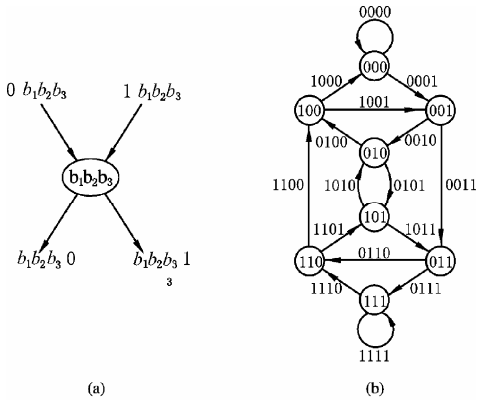


图 5.22　与图 5.21 的模数鼓轮对应的图

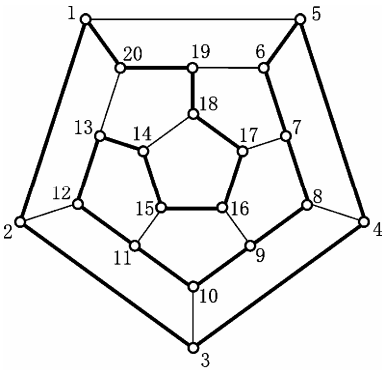


图 5.23　哈密顿图

5.6.3　哈密顿图

哈密顿图讨论的是初等路和初等回路。

1859 年，哈密顿爵士（Sir　Willian Hamilton）在与朋友的通信中提到这样一个问题，设想有一个由 12 片五边形皮子拼接成的皮球，将其中一片割去后，设想将所余部分展开成一个平面图形（如图 5.23 所示，就像我们用鱼眼镜头在割去了那块皮子后形成的孔的边缘对准球内拍到的照片）。现在将图中每一顶点看成一个城市，问题是是否可以从一个城市出发，遍历所有城市又不重复通过任何一个城市而返回原地呢？对于图 5.23，这样的巡游路线是存在的，它以粗实线描绘了出来。

定义 5.30　在一个无向图中，若存在一条通过所有结点的初等路，则称此为**哈密顿路**。若存在通过所有结点的初等回路，则称此为**哈密顿回路**，含有哈密顿回路的图叫做**哈密顿图**。

进一步要问，是否存在哈密顿图的充要条件呢？很遗憾，至今还没有人直接给出过这个充要条件。本节仅给出哈密顿图的一个充分条件和一个必要条件。

下面是一个哈密顿图的必要条件。

定理 5.10　无向图 $G=<V,E>$ 是哈密顿图，对于 V 的任意一个非空子集 $S\subseteq V$，若以 $|S|$ 表示 S 中顶点的数目，$G-S$ 表示从 G 中删除了 S 中所有点以及所有关联于这些点的边后得到的子图，则有

$$w(G-S)\leqslant|S| \tag{5.12}$$

其中 $w(G-S)$ 表示子图 $G-S$ 的连通分支数[*]。

证明　设 C 是 G 的一条哈密顿回路。因为 C 通过 G 的所有结点，若从 C 中删去某一结点 v_1 以及与之关联的两条边之后，所得子图 C' 仍是连通的，即 $w(C-\{v_1\})=1$。显然，$w(C-\{v_1\})\leqslant|S|=1$ 成立。再次从 C' 中删去一点 v_2 以及与之关联的边之后，得到子图

[*] 一个无向图的连通分支数就是该图的所有连通分图的数目。一个无向连通图本身就是一个连通分图，所以，其连通分支数为 1。参阅本章 5.2 节关于无向图的连通分图的说明。

$C''=C-\{v_1,v_2\}$(或$C''=\{C_1-\{v_2\}\}$)至多有 2 个连通分支，即$w(C-\{v_1,v_2\})\leqslant|S|$仍成立。由归纳法可证明，一般地有

$$w(C-S)\leqslant|S|$$

又因为C是G的子图，所以，显然

$$w(G-S)\leqslant w(C-S)$$

从以上两不等式可推知最终结果。

这个定理常用来论证一个无向图不是哈密顿图。就是说，如果对某一图G给出一个不满足式（5.12）的实例，则可断言G不是哈密顿图。请读者切记，由于式（5.12）只是哈密顿图的必要而非充分条件，所以，满足该式的图也可能不是哈密顿图。我们在图 5.24 中给出了两个这样的例子。第一个是由两个孤点组成的极其简单的图。很明显它不是哈密顿图，我们只是用它来强调即使满足式（5.12）的图也可以不是哈密顿图。另一个有同样的情形（请读者自行证明）。

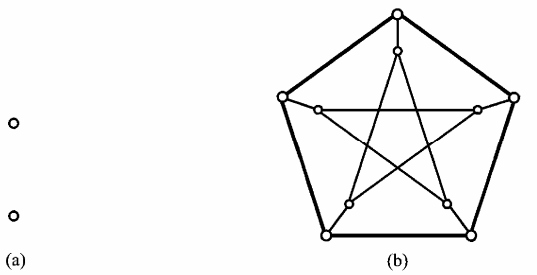


图 5.24　满足公式（5.12）的非哈密顿图

而图 5.25 给出了 3 个因不满足式（5.12）而一定不是哈密顿图的例子，在图 5.25(a)中删去v_3，在图 5.25(b)中删去v_1和v_3，在图 5.25(c)中删去v_3和v_6后即可证实。

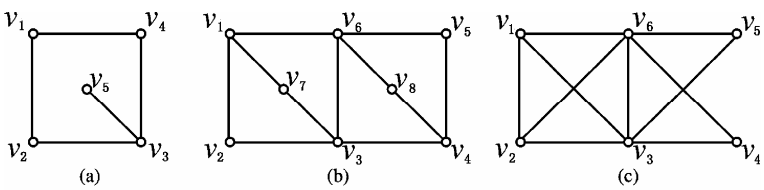


图 5.25　不满足公式（5.12）的非哈密顿图

以下是一个哈密顿图的充分条件。

定理 5.11　设G是一个不含自回路的简单无向图，有n个结点。若G的任意两个不同结点的度数之和均不小于$n-1$，则G必有哈密顿路。又若G的任意两个不同结点的度数之和不小于n，则G含有哈密顿回路。

本定理的证明较烦琐，我们不在这里给出它的证明了。

由于定理 5.11 只是哈密顿图的充分而非必要条件，所以不能用此定理判断一个图不是哈密顿图。图 5.26 给出了两个这样的例子，它们都不满足定理 5.11 的假设，但却都是哈密顿图。

【例 5.1】　有n（$n\geqslant4$）个人，若其中任意$n-2$人中的每一人至少是其余 2 人之一的朋友。试证明安排这n个人沿一圆桌就餐，使每一人的两侧都是他的朋友是可能的。

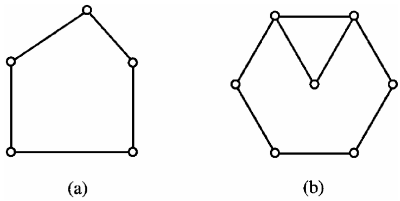


图 5.26　哈密顿图

证明　用一无向图 G 表示这 n 个人间的朋友关系。即以 n 个结点表示 n 个人，两个结点之间有一条边，当且仅当对应的这两人是朋友。可证明，在假设条件下，任两个不同结点的度之和均不小于 n，由定理 5.11 可知 G 含有哈密顿回路。显然，此回路上结点的次序正是一个满足题目要求的座位安排方案。

设 u,v 是图 G 的任意两结点，若它们是朋友，则按题设该两点度数之和大于等于 n（见图 5.27(a)）。若 u 和 v 并不相识，按照题设，对其余 $n-2$ 人中的某一人 w，他至少是 u 或 v 之一的朋友。为明确起见，设 u 和 w 是朋友。因为 u,w 两人中，已假设 u 不是 v 的朋友，所以 w 一定是 v 的朋友。这就是说 u,w 和 v,w 之间均各有一边。注意到 $n \geqslant 4$，所以同样可论证在 u,v 之外，还有另一点 t，他是 u 和 v 共同的朋友（见图 5.27(b)）。显然，同样也证明了 u,v 度数之和大于等于 n。

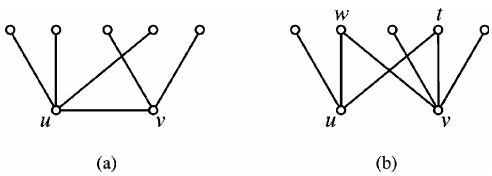


图 5.27　例 5.1

要说明的是图 5.27 并没有完整地画出图 G 来，我们省略了许多在上述讨论中没有涉及的边。

5.7　最短路径与最长路径问题

最短路径与最长路径是图论中两个很有用的专题。对于前者，我们的讨论针对无向图进行，但对有向图而言一切讨论仍是有效的。后者是一个建立在有向图基础上的问题。

5.7.1　最短路径

如图 5.28（a）给出了一个加权无向图 $G=<V,E,w>$。假如它的顶点表示 6 个城镇，关联于它们的各边表示连接它们的公路，而每一边的边权可以有各种解释。例如，边权表示该公路的里程数，或公路的通行费，或者是公路上每月平均的交通肇事次数等等。于是我们可以问这样的问题，如果从某一城镇（如 v_0 城）出发，到其余各城的最短里程是怎样的？或者是缴纳的通行费最少的路线是怎样的？或者是最安全的旅行路线是什么？容易明白，这些问题都对应同一图的同一个问题，就是从某城出发，到其余各城的边权之和最小的（而不一定是边数最少的）路径是什么。最短路径因此而得名。

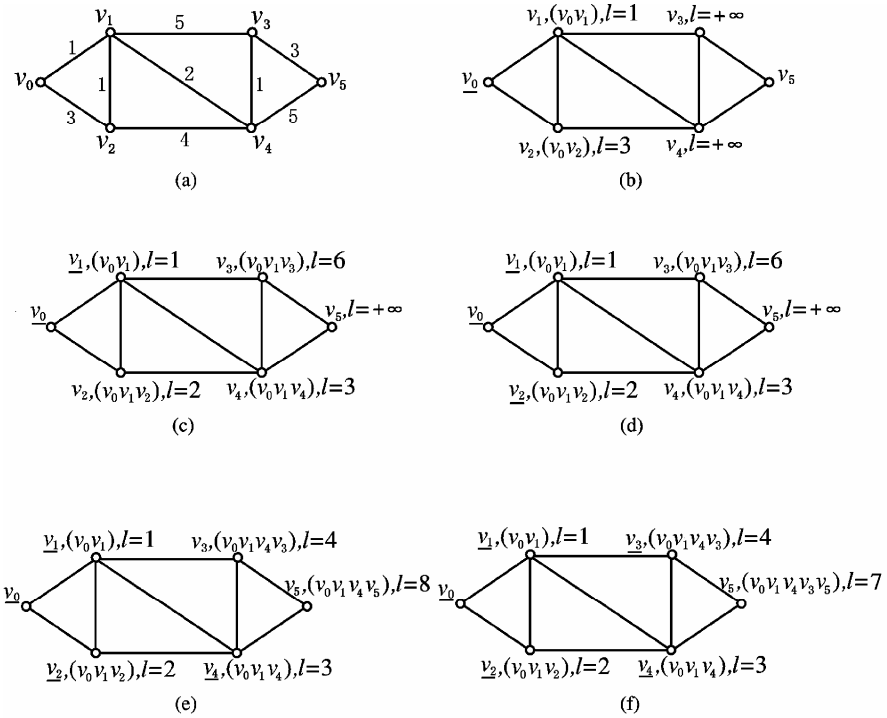


图 5.28　最短路径问题

下面是狄克斯特尔（E.W.Dijkstra）在 1959 年发表的一个求最短路径的算法。其主要思想可归纳为以下诸要点。

今假设从某一加权图的结点 v_0 出发，要求它到其余各顶点的最短路径。

1．以 U 表示所有这样的结点的集合：即结点 $v \in U$，当且仅当从起点 v_0 到这点 v 的最短路径是已求得的。显然，一开始时，$U=\{v_0\}$。

再以 S 表示图 G 中除属于 U 以外的一切结点，即 $S=V-U$。属于 S 中的每一点，从起点 v_0 到它的最短路径是待求的。

2．初始时，为每一结点 $s \in S$ 赋予一个指数 $l(s)$。一个结点 s 的指数与从 v_0 到 s 的某一种特殊结构的路有关。为陈述方便，我们称之为**“有效路”**（取其对应用 Dijkstra 方法解决最短路径是有效的意思）。有效路是这样类型的路径：$P_v=(v_0, v_{i_1}, \cdots, v_{i_t}, s)$，其中 $s \in S$，$v_0, v_{i_1}, \cdots, v_{i_t} \in U$。即只有路径的终点 s 本身落在集合 S 中，其余各点均属于集合 U。于是，结点 $s \in S$ 的指数 $l(s)$ 定义为所有这样的有效路（而不是所有 v_0 到 s 的路）中边权之和最小的那条的边权之和。即

$$l(s)=\min\{(v_0, v_{i_1}, \cdots, v_{i_t}, s)\text{的边权之和} \mid v_0, v_{i_1}, \cdots, v_{i_t} \in U, s \in S\} \tag{5.13}$$

回过去看图 5.28（b）。一开始，我们自然地将起点 v_0 归于集合 U（在属于 U 的结点名字下加下划线表示）。于是 v_0 到 v_1, v_2（$v_1, v_2 \in S$）各只有一条有效路（虽然还有 $(v_0, v_2, v_1), (v_0, v_1, v_2)$ 等等，但是这些都不是有效路），它们就是边 (v_0, v_1) 和 (v_0, v_2)。所以此时它们的边权 1 和 3 就是它们的指数：$l(v_1)=1$，$l(v_2)=3$。其余各点的指数为＋∞（想一想，为什么？）。

3. 对于 $s \in S$ 的每一点，指数 $l(s)$ 并不一定就是到它的最短路径（记住这一点非常重要!）。因为可能有另一条不属于有效路的路径，它包含了除 s 自己以外的另一点 $s' \in S$，并且该路径边权之和比指数 $l(s)$ 更小。如图 5.28(b)这一步骤上，$l(v_2)$=3，但观察发现路径(v_0, v_1, v_3)（这是一条非有效路）的边权之和仅为 2（此时 $v_1 \in S$），比 $l(v_2)$ 小。但是这并不重要，随着计算的进行，这条对结点 v_2 是真正的最短路径(v_0, v_1, v_3)，总会在计算的某一步上成为当时最短的有效路并且被选中作为 v_2 的最短路径的。重要的是对所有 S 中的结点 $s \in S$，若以 $\bar{s}$ 表示属于 S 的所有点中指数最小的一个：

$$l(\bar{s}) = \min\{l(s), s \in S\} \qquad (5.14)$$

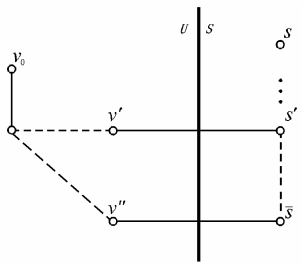


图 5.29　最短路径的证明

那么，v_0 到这个具有最小指数的点 $\bar{s}$ 的最短路径，就是那条给 $\bar{s}$ 以该指数的有效路径。或者说，$\bar{s}$ 的最短路径的边权之和（记住以下我们称一条路的边权之和为它的“长度”）就是从起点 v_0 到 $\bar{s}$ 的最短有效路的长度，它等于指数 $l(\bar{s})$。证明如图 5.29 所示。

设 $\bar{s} \in S$ 满足式（5.14）。要证明 $l(\bar{s})$ 等于 v_0 到它的最短路径的长度。

若不然，另外还有一条到 $\bar{s}$ 的路 P'，且 P'的长度 $< l(\bar{s})$，显然，P' 一定不是有效路（因指数 $l(\bar{s})$ 是所有到 $\bar{s}$ 的有效路中长度最小的一个）。那么 P' 必含有除 $\bar{s}$ 以外的另一点 $s' \in S$，设 P'=($v_0, \cdots, v', s', \cdots, \bar{s}$)。我们假设 s' 是从 v_0 出发到 $\bar{s}$ 的路径 P' 上第一个出现的属于集合 S 的点。将 P' 分成两部分：($v_0, \cdots, s'$)和($s', \cdots, \bar{s}$)。前者的长度大于等于 $l(s')$，后者的长度大于等于 0（记住权值是非负实数）。就是说 P' 的长度大于等于 $l(s')$。即 P' 长度 $\geqslant l(s') \geqslant l(\bar{s})$（因 $l(\bar{s})$ 是当前所有指数中最小的）。于是，P' 的长度 $\geqslant l(\bar{s})$。与反证法假设矛盾。证完。

我们将以上的论述小结一下。在求解最短路径的每一步上，对于每一 $s \in S$,$l(s)$ 只是 v_0到s所有有效路中长度最短的那条的边权之和，不一定是它的最短路的长度；每一个 $s \in S$ 都有一个指数 $l(s)$，它是一切从起点到 s 的有效路中最短的；其中最小的一个指数是 $l(\bar{s})$，只有结点 $\bar{s}$ 的最短路的长度才等于 $l(\bar{s})$，并且最短路就是形成该指数 $l(\bar{s})$ 的有效路。

4．当我们在每一步骤上求得集合 S 中一个指数最小的结点 $\bar{s} \in S$ 之后，就将它纳入集合 U 中去。即 $U \leftarrow U \cup \{\bar{s}\}$，$S \leftarrow S - \{\bar{s}\}$。如图 5.28（c）是将 v_1 纳入 U 之后的情况。这样，$U = \{v_0, v_1\}$。可以看出，这时 $v_2 \in S$，除原有的一条有效路（(v_0, v_2)，其长度是 3）以外，又有一条新的有效路(v_0, v_1, v_2)。后者正是因为我们将 v_1 纳入了集合 U 之后新出现的。当然，我们有理由在“新情况”下，重新评估留在集合 S 中的各点的指数。对 v_2 而言，因新出现的有效路(v_0, v_1, v_2)的长度比老的指数 $l(v_2)$ 更小，所以就需用这个更短的有效路的长度取代其老的指数。注意，一般而言，每当将一个指数最小的点 $\bar{s} \in S$ 加入 U 之后，对剩下在 S 中的各点可能出现的新的有效路至多有一条，其长度为指数 $l(\bar{s})$ 与边($\bar{s}$,s)的边权之和 $l(\bar{s}) + w((\bar{s}, s))$。因此，每次产生 $\bar{s}$ 并加入集合 U 之后，余留在 S ($S \leftarrow S - \{\bar{s}\}$)中的点 $s \in S$ 的新指数 $l'(s)$ 需按下式修改

$$l'(s) = \min\{l(s), l(\bar{s}) + w((\bar{s}, s))\} \qquad (5.15)$$

其中 $\bar{s}$ 是最近一次从 S 中选出的具有最小指数 $l(\bar{s})$ 的点（参考图 5.30（a））。$l(s)$ 是属于 S 的点在 $\bar{s}$ 未加入 U 之前的老指数，$l'(s)$是同一些点在将 $\bar{s}$ 加入 U 之后的新指数（参照图 5.30（b））。

$w((\bar{s},s))$是边$(\bar{s},s)$的权。返回到图 5.28（c），加入了 v_1 以后，新的指数 $l'(v_2)=\min\{l(v_2), l(v_1)+w((v_1,v_2))\}=\min\{3,1+1\}=2$, $l'(v_3)=\min\{l(v_3), l(v_1)+w((v_1, v_3))\}=\min\{+\infty, 1+5\}=6$……

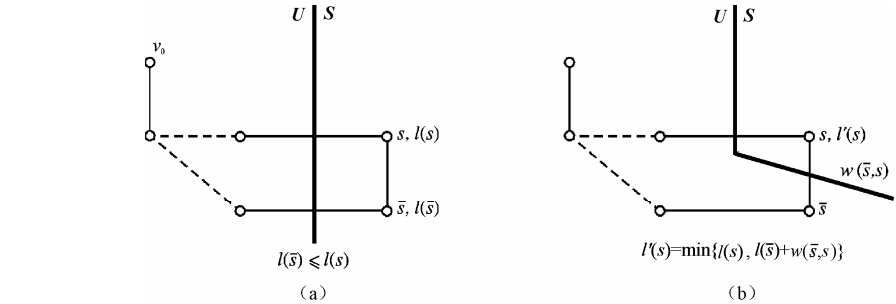


图 5.30　指数 $l(s)$ 的修正

归纳以上要点，狄克斯特尔的算法如下：

设 $G=<V,E,w>$ 是一加权无向图，v_0 是起点。

（1）初始化。$U\leftarrow\{v_0\}$，$S\leftarrow(V-U)$。若 $S=\phi$，结束。否则对 $s\in S$,计算$l(s)$。

（2）求 $\bar{s}\in S$，使之满足 $l(\bar{s})=\min\{l(s), s\in S\}$。$U\leftarrow(U\bigcup\{\bar{s}\})$, $S\leftarrow(S-\{\bar{s}\})$。

（3）若 $S=\phi$，则结束。否则修改 $s\in S$ 的指数。$l(s)\leftarrow l(s)=\min\{l(s), l(\bar{s})+w(\bar{s},s)\}$。返回第（2）步。

顺便说一句，从以上算法可知，到各结点的最短路是循着从小到大的次序逐一求得的。

5.7.2　最长路径

设有一大的工程 P，由若干个子工程 p_i 组成。并且，各子工程的进程客观上遵循一个先后次序。就是说，某子工程 p_k 必须在另一个或一些子工程全部完成之后方可开始。我们可以以一条有向边表示一项子工程，并且如果该子工程必须在子工程 p_i, p_j 均完成后方可开工，则我们将边 p_i, p_j 汇集至一点 v_r，并从 v_r 引出边 p_k（如图 5.31（a））。

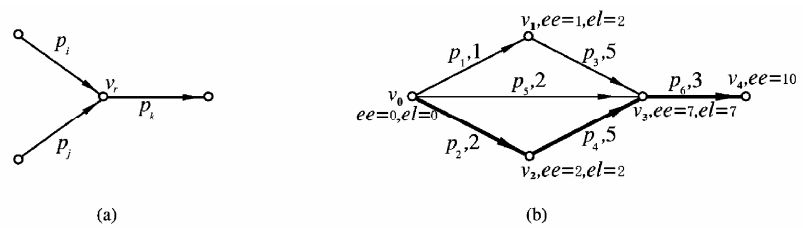


图 5.31　简单评审图

图 5.31(b)给出了一个由 6 个子工程组成的很简单的有向图。它描述了该工程的各子工程之间的**时序**关系。其中每一边的边权表示该子工程的预期工期，设以“天”为单位。这样的加权有向图，通常称为**评审图**。从中我们可以看出，最后一子工程 p_6 完成后，全部工程完工。所以又将出度为 0 的结点 v_4 叫做收点。往后追溯，p_6 的开工必须是在 p_3, p_4 和 p_5 都完工之后。结点 v_3 就表示 p_3, p_4 和 p_5 三者较晚完工的那一子工程结束的时刻，所以 v_3 也叫做一事件。同样 p_3 的开工，必须等待 p_1 的完工，p_4 的开工要等到 p_2 完工。最后，结点 v_0 是一入度为 0 的点，它表示整个工程开始的时刻，所以 v_0 又叫发点。因此可知，p_6 可以开工的时间受

制于 p_1, p_2, p_3, p_4, p_5 的进度。我们要问， p_6 最早可在整个工程开始后的第几天开工呢？从以上分析不难知道， v_3 表示的事件发生之时，代表 p_1, p_2, p_3, p_4, p_5 这 5 个子工程全部完工的时刻。于是，从发点 v_0 开始计时，完成 p_1, p_3 需要 1+5=6（天），而完成 p_2, p_4 需要 2+5=7（天），完成 p_5 需 2（天）。显然， v_3 的出现是在开工之后第 7 天，也即这时 p_6 才可开工。由此不难算出，收点 v_4 的发生（全部完工），至少要到开工之后的 $(p_2)+(p_4)+(p_6)=2+5+3=10$（天）。请注意， v_3 的最早出现时间是一条从发点开始至 v_3 的最长路径（边权之和最大，下同），同样 v_4 的最早发生时间是一条从发点至收点的最长路径（这条最长路径上的边在图 5.31 (b) 中以粗实线标记了出来）。现在我们可以说，一个评审图中的任一结点对应一个事件，而该事件发生后，那些从它引出的边表示的子工程才可开始。而该事件发生的时刻对应了从发点开始到这个结点的所有有向路中最长一条的边权之和。这也是为什么我们把讨论评审图的问题叫做**最长路径问题**的道理。

下面是一些讨论评审图时经常用到的术语。

发点：是评审图中入度为 0 的点。评审图通常只有一个入度为 0 的结点。若有多于一个入度为 0 的点，我们可以重新建立一个发点，由它引出若干边权为 0 或大于 0 的边至上述各入度为 0 的结点（如果这些结点并不同时并工的话）。

收点：是出度为 0 的结点，表示所有子工程均结束的时刻。

活动或**子工程**：一个工程中相对独立的进程，用图的一条有向边来表示之。边权是该进程的时间。

事件：用一结点表示一事件。它对应某一时刻，该时刻的到来，意味着一切从发点至该结点的所有路径上的活动全部完成。

事件的最早发生时刻：用 $ee(v_i)$ 表示从开工时刻计时，事件 v_i 最早发生（出现）的时刻。每一个事件（包含收点）的最早发生时刻等于从发点至该事件的所有路径中最长一条的边权之和。也即这些路径上的所有活动（边）都完成的最早时刻（参见图 5.31（b））。

约定，发点的最早发生时刻为 0（计时起点）。即

$$ee(\text{发点}) = 0 \tag{5.16}$$

事件的最迟发生时刻：用 $el(v_i)$ 表示在不延误收点的最早发生时刻的前提下，从开工时刻计时，某事件 v_i 可最迟发生的时刻。显然， $el(v_i)$ 等于收点的最早发生时间（整个工程完成所需的时间）与 v_i 至收点的所有路径中最长者的边权之和的差（参考图 5.31（b）中 v_1 的 el ）。

由于收点是整个工程结束的时刻，所以我们约定收点的 ee 值等于 el 值，即

$$ee\,(\text{收点}) = el\,(\text{收点}) \tag{5.17}$$

活动的最早发生时刻：活动 $<v_i, v_j>$ 的最早发生时刻显然等于其起点 v_i 的最早发生时刻 $ee(v_i)$ 。活动的最早发生时刻用 $ae(<v_i, v_j>)$ 表示之，有

$$ae(<v_i, v_j>) = ee(v_i) \tag{5.18}$$

活动的最迟发生时刻：用 $al(<v_i, v_j>)$ 表示之。它等于在不延误收点的最早发生时刻的前提下，活动$<v_i, v_j>$可最迟开始的时刻。显然，它等于该活动的终点的最迟发生时刻与该活动所需时间（即边权）之差，即

$$al(<v_i, v_j>) = el(v_j) - w(<v_i, v_j>) \tag{5.19}$$

关键活动：边$<v_i, v_j>$是关键活动，当且仅当其最早发生时刻等于其最迟发生时刻，即

$ae(<v_i,v_j>)=al(<v_i,v_j>)$。

关键路径：从发点至收点的一条全部由关键活动组成的路径。

从以上定义可知，关键活动的两个端点均是最早发生时间与最迟发生时间相等的事件。但是要切记，反之不然（如图 5.31（b）中的活动 p_5 ）。

要控制一个总工程的工期，主要是监控那些关键活动。它们都处于某些关键路径上。因为关键路径从某种意义上说，均是其起点和终点间的最长路径，所以其中若有一关键活动延期了（没有在其边权指定的时间内完成），那么势必影响到总工期按时完成。而那些非关键路径上的某些非关键活动则可以在一定范围内延期，也不致于影响总工期按时完成。所以，研究一个工程的评审图时，重要的是找出所有关键活动，从而也就找出了关键路径。由公式（5.18）和公式（5.19）可知，首先要求出所有事件的 *ee* 和 *el* 的值。

我们以图 5.32 给出的评审图为例来讨论如何求关键活动的方法。

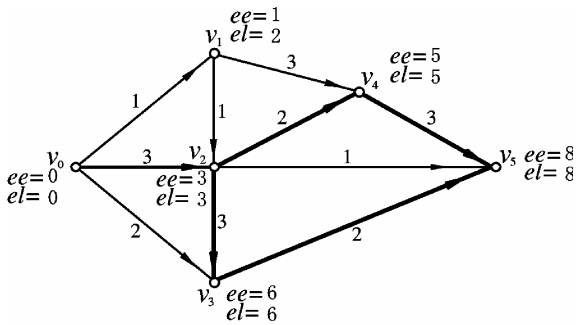


图 5.32　评审图的解

首先从发点开始，逐一向前（我们称较晚发生的事件相对较早发生事件在前方，因为历史的东西总要往“后”才能追溯到）求得每一事件的 *ee* ，直到收点。然后，从收点开始，逐步向后推出其余各事件的 *el* ，直到发点。显然，某一事件的 *ee* 值，只有在该事件的所有前驱事件的 *ee* 值均求出之后方是可解的。一事件的所有前驱事件系指从出发点开始至该事件的所有有向路径上的结点。因此，在本例中，求事件的 *ee* 值的一个次序是 v_0,v_1,v_2,v_3,v_4,v_5 。这样的序列也称为**拓扑序列**。

求 *ee* 值的步骤如下：

（1）按约定（式(5.16)），$ee(v_0)=0$。

（2）$ee(v_1)=ee(v_0)+w(<v_0,v_1>)=0+1=1$ 。

（3）$ee(v_2)=\max\{ee(v_1)+w(<v_1,v_2>),\ ee(v_0)+w(<v_0,v_2>)\}$
$=\max\{2,3\}=3$ 。

（4）$ee(v_3)=\max\{ee(v_2)+w(<v_2,v_3>),ee(v_0)+w(<v_0,v_3>)\}$
$=\max\{6,2\}=6$ 。

（5）$ee(v_4)=\max\{ee(v_1)+w(<v_1,v_4>),ee(v_2)+w(<v_2,v_4>)\}$
$=\max\{4,5\}=5$ 。

（6）$ee(v_5)=\max\{ee(v_2)+w(<v_2,v_5>),ee(v_3)+w(<v_3,v_5>),$
$ee(v_4)+w(<v_4,v_5>)\}$
$=\max\{4,8,8\}=8$。

求 *el* 值的步骤如下：

（1）按约定，收点的最早发生时刻与最迟发生时刻相等，所以 $el(v_5)=ee(v_5)=8$。

（2）$el(v_4)=el(v_5)-w(<v_4,v_5>)=8-3=5$。

（3）$el(v_3)=el(v_5)-w(<v_3,v_5>)=8-2=6$。

（4）$el(v_2)=\min\{el(v_3)-w(<v_2,v_3>),el(v_4)-w(<v_2,v_4>),el(v_5)-w(<v_2,v_5>)\}$
$=\min\{6-3,5-2,8-1\}=3$。

（5）$el(v_1)=\min\{el(v_2)-w(<v_1,v_2>),el(v_4)-w(<v_1,v_4>)\}$
$=\min\{3-1,5-3\}=2$。

（6）$el(v_0)=\min\{el(v_1)-w(<v_0,v_1>),el(v_2)-w(<v_0,v_2>),$
$el(v_3)-w(<v_0,v_3>)\}$
$=\min\{2-1,3-3,6-2\}=0$。

注意：最后求得的发点的最迟发生时间必然也等于最早发生时间的值 0。这实际上是一个回归验算。不然就说明在计算中有错误。

最后将所有结果和运用公式（5.18）及公式（5.19）计算出各活动的 *ae* 值和 *al* 值列在表 5.2 中。

表 5.2　*ae* 值和 *al* 值

事件	*ee*	*el*	活动	*ae*	*al*	*ae*=*al*？
v_0	0	0	$<v_0,v_1>$	0	1	
v_1	1	2	$<v_0,v_2>$	0	0	√
v_2	3	3	$<v_0,v_3>$	0	4	
v_3	6	6	$<v_1,v_2>$	1	2	
v_4	5	5	$<v_1,v_4>$	1	2	
v_5	8	8	$<v_2,v_3>$	3	3	√
			$<v_2,v_4>$	3	3	√
			$<v_2,v_5>$	3	7	
			$<v_3,v_5>$	6	6	√
			$<v_4,v_5>$	5	5	√

回到图 5.32，所有粗实线表示的边是关键活动，可见该评审图有两条“平行”的关键路径。请读者分析一下，哪些关键活动提前完工（所用时间少于其边权）可使整个工程提前完工？在其他活动完工时间不变的条件下，提前完成这些关键活动至多可使总工期提前多少时间（收点的 *ee* 值最多可提前多少）？又请问，哪些关键活动提前完工不能使总工期提前完成呢？

5.8　平面图

平面图的图形有一些特殊的性质，它在管线的敷设、交通道路设计和印刷电路板的设计上有直接的应用。

定义 5.31　设 $G=<V,E>$ 是一无向图。若能够将它画在一个平面上并使所有边除在结点以外的任何地方均不相交，则 G 就是一个**平面图**。

图 5.33（a）是平面图，看似不是平面图的图 5.33（b）可以画成图 5.33（c）或图 5.33（d）那样证实它实际上是一个平面图。所以，问题在于如何证明一个平面图，而不在于是否可以将一个平面图的图形画出来。

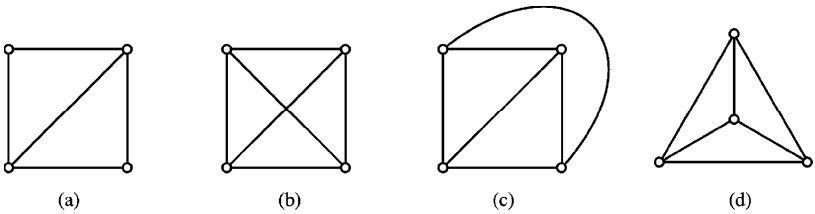


图 5.33　平面图的例子

再来看图 5.34。其中图 5.34（a）是完全图 K_5。图 5.34（b）对应一个著名的问题，就是为三所房子的每一座都安装 w,g,e 三种公用管线而使得没有任何两根管线是相交的设计。稍后，我们来证明图 5.34 的两个图形都不是平面图。

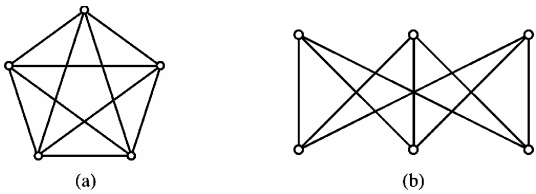


图 5.34　两个典型的非平面图

定义 5.32　在一个平面图中，一个或若干个回路 *共同包围的平面区域，并且该区域内不再包含回路围出的子区域，则该平面区域叫做是平面图的一个**面**。围出一个面的回路叫**边界**。

若一个面可以被充分大的一个圆所包含，则称此面是**有限面**，否则称为**无限面**。

容易明白，一个平面图恰有一个无限面。

沿着一个面的边界巡行有两个方向，如果沿某一方向巡行时，该面最接近巡行者的那部分总出现在巡行者的左侧，则这个方向叫做边界的正方向；这实际上是按**右定向法则**为平面建立了一种方向，即以指向巡行者头部的平面法线来确定平面的（正）方向。若一个平面有多个边界，则包含其余所有边界的那一个叫做**外部边界**，如图 5.35（d）中的 C_1；其余的边界都叫做**内部边界**，如图 5.35（d）中的边界 C_2 和 C_3。

图 5.35（a）中，面 P_1 有一条外边界 C_1 和两条内边界 C_2, C_3（后两者正方向是“顺时针方向”）。同时，C_2, C_3 又各是面 P_2, P_3 的外边界（其正方向是“逆时针方向”）。当一个面的内、外边界被一条路连通后，则内、外边界合而为一，就成了一条外边界，如图 5.35（b）。对于无限面的情况下，设想其外边界在无限远处，无限面的所有边界都是内部边界，如图 5.35（c）中无限面 P_3 有两条内部边界 C_1 和 C_2。

定义 5.33　遍历平面图 P 的边界时，所通过的边数叫做该面的**度**，记做 $\deg(P)$。

在图 5.35（a）中，$\deg(P_1)=11$，$\deg(P_2)=4$，$\deg(P_3)=3$，$\deg(P_4)=4$。在图 5.35（b）中，$\deg(P_1)=7$。因为要完整地绕行它的边界一周，必须两次通过边 e。

定理 5.12　有限平面图 $G=<V,E>$ 的所有面的度数之和等于此平面图总边数的 2 倍。即

$$\sum_{P_i \in P(G)} \deg(P_i) = 2|E| \qquad (5.20)$$

* 这里的回路同本章 5.4.1 小节类似，排除一条无向边作为回路的情况，但不排除平行边围成的回路。

其中 $P(G)$ 是图 G 所有面的集合。

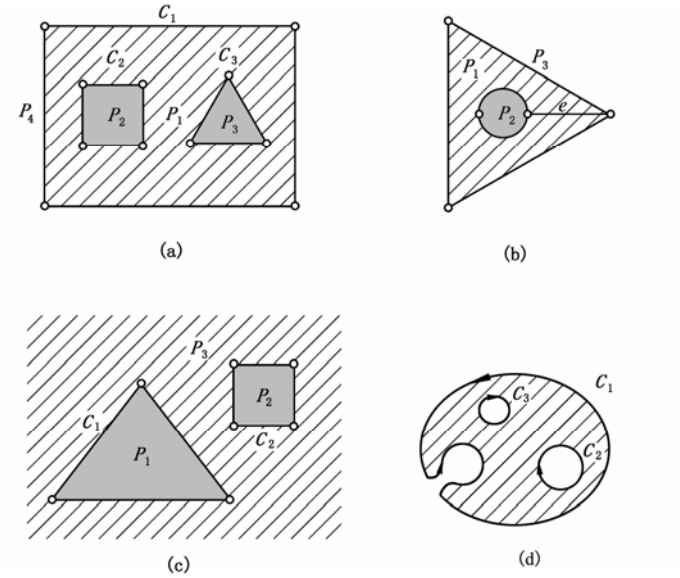


图 5.35　面和边界

证明

边界上的边可分成两类，一类是边的两侧分属两个不同的面，它为每一面提供各 1 度。另一类是边的两侧属同一面，如图 5.35(b)中 P_1 的边 e，它为一个面供应 2 度。总之，每一边为一个平面图各个面的总度数贡献 2 度。证明完毕。

若一个平面图是连通图，称此平面图为**平面连通图**。平面连通图有着重要的性质。

定理 5.13　设平面连通图 G 有 v 个顶点、e 条边和 p 个面，则以下公式成立

$$v-e+p=2 \tag{5.21}$$

这个定理又被叫做**欧拉定理**。它对任何凸多面体也成立。

证明　我们用归纳法来完成这个定理的证明。

归纳基础：一个仅含一条边的或不含边的连通图满足公式（5.21）（见图 5.36）。

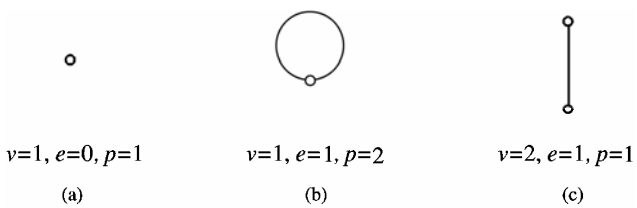


图 5.36　满足欧拉定理的最简单平面图

归纳步骤：假设具有 $k-1$ 条边的平面连通图满足式（5.21）。又设 G 是具有 k 条边的平面连通图。如果 G 含有 1 度结点，删除这个结点和关联于它的一边，则成为一个有 $k-1$ 条边的平面连通图 G'。所以按归纳法假设 G' 满足式（5.21）。再将 G' 上添入刚刚被删去的一条边和一个顶点，则得原来有 k 条边的平面连通图。显然它仍满足公式（5.21）。

若 G 原来不含有 1 度的结点，可以证明 G 必有有限面。若删除某有限面边界上的一条边，得到子图 G' 仍是连通的。G' 满足公式（5.21），当加入刚刚被删去的那一边之后，图的边数 e

加 1，而它的面数也加 1，故公式（5.21）仍是成立的。

定理 5.14 边数大于等于 2 的无自回路的简单平面连通图，其结点数 v 和边数 e 满足以下公式

$$e \leqslant 3v-6 \tag{5.22}$$

证明 该定理实际上对非连通平面图也是对的。首先从连通平面图开始我们的证明。

由于假设平面连通图无自回路和平行边，所以平面图的每一面 P_i 的度 $\deg(P_i) \geqslant 3$（参看图 5.37 给出的几种情况，注意其中(a),(b)每一边对相关面贡献 2 度），所以，平面图各面度数之和 $\sum_{P_i \in P(G)} \deg(P_i) \geq 3p$，$p$ 表示面的数目。另外，$\sum_{P_i \in P(G)} \deg(P_i) = 2e$，所以

$$2e \geqslant 3p \quad 或 \quad p \leqslant \frac{2}{3}e$$

联系欧拉公式（5.21），整理后有

$$\frac{e}{3} \leqslant v-2 \quad 或 \quad e \leqslant 3v-6$$

最后，在不连通平面图的情况，设它有 n 个连通分支 *。现在用 $n-1$ 条边将所有连通分支两两连成一个连通图，所得新的连通平面图满足式（5.22）。删去刚才加上的 $n-1$ 边之后得到原来平面图。这样就在总边数中减去了 $n-1$，同时结点数并未减少，故公式（5.22）仍是成立的。

特别提醒读者注意，欧拉公式（5.21）和公式（5.22）各自成立的前提。欧拉公式要求平面图必须是连通的，但从证明过程可见，并不要求平面图中无自回路和平行边；而公式（5.22）则相反，并不要求平面图连通，但却要求图中不含自回路和平行边。

【例 5.2】 证明完全图 K_5 不是平面图。

证明 K_5 中含有 5 个结点 $v=5$ 和 10 条边 $e=10$。它不满足不等式（5.22），所以 K_5 不是平面图。

【例 5.3】 证明图 5.34(b)给出的图不是平面图（此图也称为 $K_{3,3}$ 图）。

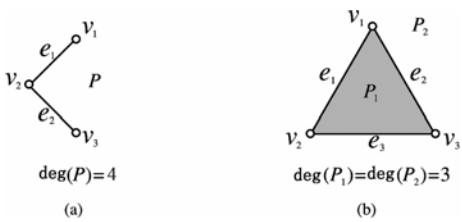


图 5.37 一些边界的边数不少于 3 的平面连通图

证明 反证法。

若不然，设 $K_{3,3}$ 是平面图。由于从 $K_{3,3}$ 中任取 3 个不同顶点，至少有两个是不相邻的，所以它每一面的度不小于 4（也即其中不含长度小于 4 的回路）。以 p,v,e 分别表示 $K_{3,3}$ 的面数、顶点数和边数。有

$$4p \leqslant 2e \qquad 或 \qquad p \leqslant \frac{1}{2}e$$

* 参阅本章关于定理 5.10 的脚注。

与欧拉公式（5.21）一起，解得

$$2v-e\geqslant 4$$

但 $K_{3,3}$ 的 $v=6, e=9$，不满足以上不等式。矛盾。

最后是一个平面图的充要条件，1930 年，由库拉多夫斯基（Kuratowski）给出。

若在一无向图 G 中，以一条除端点外均是 2 度的初等路代替 G 中一条边后，生成图 G'。显然 G 和 G' 是否为平面图与这样的替代无关（见图 5.38）。

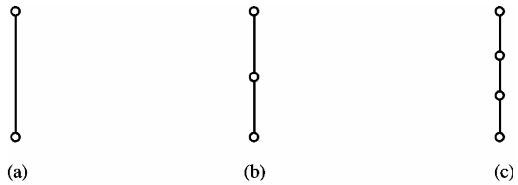


图 5.38　同胚的边

定义 5.34　设 G 是无向图。若在 G 的一条边上，两端点间插入 $k\geqslant 0$ 个新结点使之成为一条长度是 $k+1$ 的初等路，从而生成 G'；或者正相反，以一条边代替 G 的两端点间的一条初等路，并且该初等路的中间结点均为 2 度的，从而生成图 G''。这样，我们就说图 G 和 G' 或 G 和 G'' 有**同胚的边**，并称 G 和 G' 或 G 和 G'' 是同胚的。

图 5.39 中（a）与（b）同胚，（c）与（d）同胚。

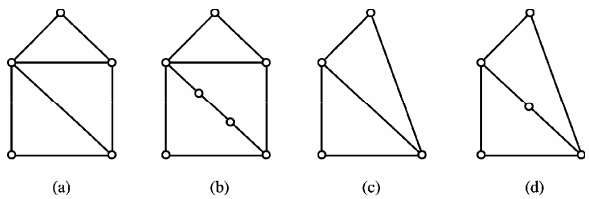


图 5.39　同胚的图

以上已经证明了 K_5 和 $K_{3,3}$ 均不是平面图。所以若图 G 有与 K_5 或 $K_{3,3}$ 同胚的子图，则 G 本身一定不是平面图。库拉多夫斯基还证明了非平面图一定含有与 K_5 或 $K_{3,3}$ 同胚的子图。

定理 5.15　一个无向图是平面图，当且仅当它不含有与 K_5 或 $K_{3,3}$ 同胚的子图。

这就是库拉多夫斯基（Kuratowski）定理。

习　　题

5.1　证明任何有向完全图各结点入度的平方和等于出度的平方和。

5.2　给出图 5.40 的补图。

5.3　给出图 5.41 中（b）所示 G' 相对于（a）所示图 G 的补图 G''。问 G' 是否也是 G'' 相对于 G 的补图？为什么？

5.4　证明图 5.42 中两个图是同构的。

5.5　一个图若同构于它的补图，则称该图为自补图。

（a）给出一个 5 个结点的自补图。

（b）是否存在 3 个结点与 6 个结点的自补图？为什么？

（c）图 G 有自补图的必要条件是什么？

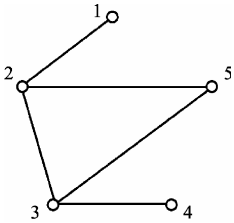


图 5.40　习题 5.2

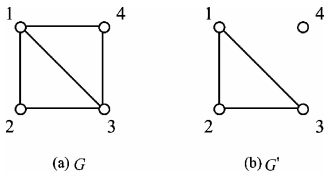


图 5.41　习题 5.3

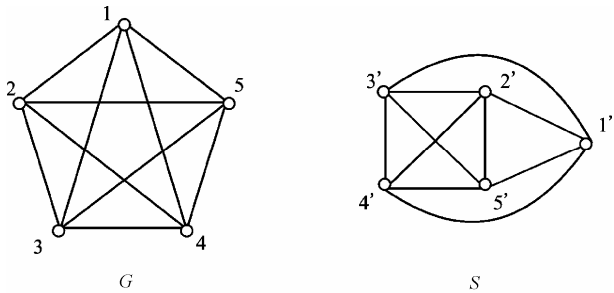


图 5.42　习题 5.4

5.6　证明：若无向图 G 是不连通的，则它的补图是连通的。反之，若 G 是连通的，那么 $\overline{G}$ 是否一定不连通？说明之。

5.7　给出一有向图，如图 5.43 所示。求结点 v_1 到 v_4 之间的所有简单路和初等路，并给出每一结点的出度、入度和度。最后求出距离 $d<v_1,v_4>$ 和 $d<v_5,v_2>$。

5.8　图 5.44 给出了一个有向图。试求出它的所有强分图、单侧分图和弱分图。

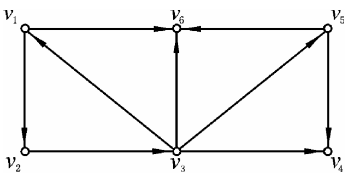


图 5.43　习题 5.7

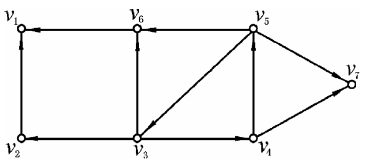


图 5.44　习题 5.8

5.9　证明：有向图是单侧连通的充分必要条件是存在一个包含图的所有结点的路。

5.10　证明：无向图两结点的连通性是结点集上的等价关系。由这个等价关系所诱导的等价类有何具体意义？

5.11　求出图 5.43 的邻接矩阵 A，并通过计算 A 的矩阵的普通乘幂 A^2, A^3 …回答以下问题：

（a）有几条从结点 v_1 到 v_4 长度不大于 5 的路？

（b）经过结点 v_1 有没有回路？其中有没有长度为 5 的回路？

（c）求出没有任何回路经过的结点。

5.12　在一个有限图里，如何利用邻接矩阵 A 求任意两结点 v_i 到 v_j 的距离 $d<v_i,v_j>$？并应用这个方法求图 5.43 中的 $d<v_2,v_4>$ 和 $d<v_2,v_6>$。

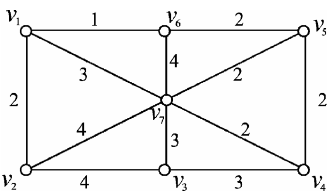


图 5.45　习题 5.13

5.13　在图 5.45 中，将每一边旁边标注的数字看成是该边的边权，试写出它以权表示的邻接矩阵 A。若将边权解释为平行边的数目，则 A^2 的含义是什么？

5.14　求出图 5.43 给出的图的路径矩阵（要求用矩阵的布尔积计算）。

5.15　设一无向树有两个 2 度结点、一个 3 度结点和三个 4 度结点。求它有多少 1 度结点？

5.16　证明：一棵无向树至少有两个 1 度结点。

5.17　证明：无向树是无回路的，且删除其任何一边后，所得的子图是不连通的。

5.18　设 T_1, T_2 是连通图 G 的两棵生成树，e 是 T_1 的边却不是 T_2 的边。证明：存在边 s，它在 T_2 中却不在 T_1 中，并使 $(T_1-\{e\})\cup\{s\}$ 和 $(T_2-\{s\})\cup\{e\}$ 都是 G 的生成树。

5.19　利用克鲁斯卡算法求图 5.45 的最小生成树。

5.20　举一简单例子说明将根树的定义写成“恰有一个结点的入度为 0，其余结点的入度均为 1 的简单有向图”，并不是我们通常定义的根树。

5.21　有多少不同构的具有 3 个结点的有向树？有多少不同构的具有 3 个结点的有序树？

5.22　如何从一个简单有向图的邻接矩阵确定一个有向图是否为一棵树？如果是根树，又如何确定它的根和叶呢？（提示：将有向边看成无向边。写出该相应无向图的邻接矩阵，结合与 5.22 定义等价的初等性质 1，判断它是否是无向树）

5.23　若一棵二权树的每一个非叶子结点的出度均为 2，则称之为完全二权树。证明：完全二权树中边数 $e=2(n_t-1)$，其中 n_t 是叶子数目。

5.24　证明：根树中任意两结点如果存在路，则只有唯一一条初等路。

5.25　试通过二权树为字母集 $\{a,b,c,d,e,f,g,h\}$ 编制一组前缀码。

5.26　有六个城市 $C_1, C_2, \cdots, C_6$。两市 C_i 和 $C_j(1\leqslant i\leqslant 6, 1\leqslant j\leqslant 6)$ 间班机旅费由以下矩阵 $P=[p_{ij}]$ 的 p_{ij} 表示。

$$P=\begin{bmatrix} 0 & 50 & \infty & 40 & 25 & 10 \\ 50 & 0 & 15 & 20 & \infty & 25 \\ \infty & 15 & 0 & 10 & 20 & \infty \\ 40 & 20 & 10 & 0 & 10 & 25 \\ 25 & \infty & 20 & 10 & 0 & 55 \\ 10 & 25 & \infty & 25 & 55 & 0 \end{bmatrix}$$

用狄克斯特算法求出从 C_1 到其余各城市旅费最少的旅行线路。

5.27　一个工程评审图的邻接矩阵给出如下。试求出该工程的所有关键路径。试问哪些工程提前完成可以使总工程提前？

$$P=\begin{bmatrix} 0 & 1 & 10 & 6 & 3 & \infty & \infty & \infty & \infty & \infty \\ \infty & 0 & 10 & \infty & \infty & 10 & \infty & \infty & \infty & \infty \\ \infty & \infty & 0 & \infty & \infty & 2 & 4 & 1 & \infty & \infty \\ \infty & \infty & 6 & 0 & 2 & \infty & \infty & 3 & \infty & \infty \\ \infty & \infty & \infty & \infty & 0 & \infty & \infty & 6 & 8 & \infty \\ \infty & \infty & \infty & \infty & \infty & 0 & 2 & \infty & \infty & 5 \\ \infty & \infty & \infty & \infty & \infty & \infty & 0 & 5 & \infty & 2 \\ \infty & \infty & \infty & \infty & \infty & \infty & \infty & 0 & \infty & 8 \\ \infty & \infty & \infty & \infty & \infty & \infty & \infty & 8 & 0 & 5 \\ \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & 0 \end{bmatrix}$$

5.28　在七桥问题中，为使问题有解，哥尼斯堡的居民至少还要修建几座桥梁？在何处建造新桥？又若为了同样的理由，至少拆除几座桥？如何拆法？

5.29　判断图 5.46 给出的两个图形是否可一笔连续画出而不在任一边重复画过？为什么？

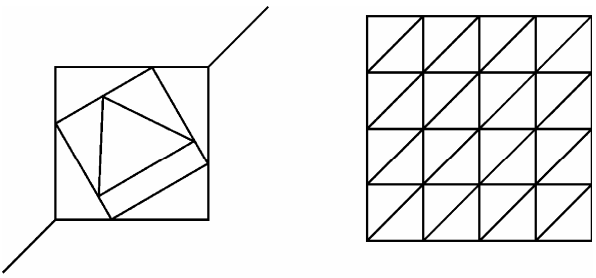


图 5.46　习题 5.29

5.30　设计一个有 8 个定位的模数鼓轮，使其能输出 8 个不同的三位二进制编码串。要求给出相应的图。

5.31　K_n 是有 n 个顶点的无向完全图。问 n 取何值时 K_n 是欧拉图？

5.32　（a）画一个有欧拉回路和哈密顿回路的图。

（b）画一个有欧拉回路但没有哈密顿回路的图。

（c）画一个没有欧拉回路但有哈密顿回路的图。

5.33　判断图 5.47 中的两个图是否是哈密顿图。说明理由。

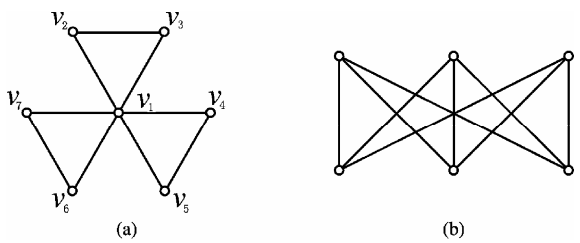


图 5.47　习题 5.33

5.34　举一例说明定理 5.11 对于有环或有平行边的图不成立。

5.35　如果为一个无向图的每一边确定一个方向，使得所得的有向图是强连通的，称该无向图是可定向的。

（a）证明欧拉图是可定向的。

（b）证明哈密顿图是可定向的。

5.36　求图 5.48 的平面图的每一个面的度数并验证公式（5.20）、公式（5.21）和公式（5.22）。

5.37　试说明 $K_5-\{e\}$ 和 $K_{3,3}-\{e'\}$ 是平面图，其中 e 和 e' 分别是 K_5 和 $K_{3,3}$ 中任意一条边。

5.38　证明：若 G 是每一面的度均大于等于 $k(k\geq 3)$ 的连通平面图，则 $e\leqslant\dfrac{k(v-2)}{k-2}$，其中 v 和 e 分别是 G 的结点数和边数。

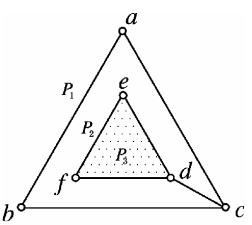


图 5.48　习题 5.36

5.39　证明边数小于 30 的无环简单平面图有一个不超过 4 度的结点。

5.40　证明：在有 6 个结点 12 条边的连通的无环简单平面图中，每个面的度为 3。

5.41　如有可能，画出图 5.49 中各图的平面图形。

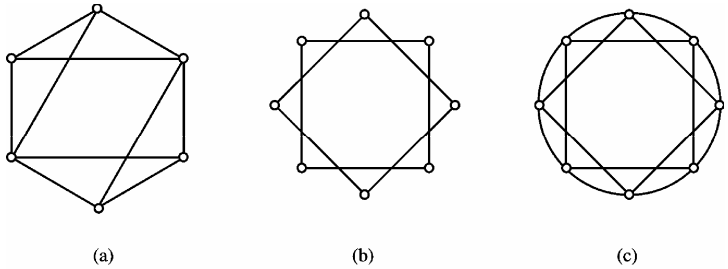


图 5.49　习题 5.41

第6章　代 数 系 统

一般地说，“**系统**”一词系指在一相对独立或封闭的环境中，一些汇聚在一起的对象的性质、行为和联系。数学上，说到系统常指具有某种性质的数学结构。在一个非空集合上，明确定义了这些元素的运算法则和运算所满足的规律。这样，我们就说该非空集合上的元素具有了一种**代数结构**或者说它们构成一个**代数系统**。

在现实世界中存在由各种具体的、各不相同的集合所构成的各自的代数系统。数学研究的是抽象的代数系统，即它的元素暂时不必赋予什么具体含义，并且抽象代数系统上的运算也只是一种函数。一旦某种抽象的代数系统的性质被证实，那么这些结论和方法将可以用于解决现实世界中某一类代数系统的问题。

在计算机科学里，形式语言、时序机理论、快速加法器和纠错码的设计等，都和代数系统的理论有关。抽象的近世代数，在计算机科学中找到了应用，反过来，后者的发展也向数学提出了新问题并促进了代数学的进一步发展。

6.1　运算和代数系统

6.1.1　运算的概念

在本书第 3 章里，我们就提到过，运算、映射和函数时常表示同一概念。我们早在小学数学教科书中，就可以学到非负整数（自然数）的加法和乘法运算。所以，运算无非是在一个非空集合上定义的一种无歧义的规则，按照此规则，非空集合的 $n(n\geqslant 0)$个元素唯一地对应某一确定的元素。该确定的元素也称为是前面那 n 个元素的运算结果。

定义 6.1　设 X 是一非空集合，一个由笛卡尔积 X^n（n=1,2,…）到集合 Y 上的 n 元函数就称为集合 X 上的一个 n **元运算**。

为使概念上统一起见，我们约定集合 X 上的某些特殊身份的元素（如整数四则运算中的 0 和 1）叫做是**零元运算**。取其运算不需要运算数（自变量），而运算结果恒等于这些特殊元素之意。

尽管从运算的定义可知，n 元运算实际上就是集合 X 到 Y 的 n 元函数（参看第 3 章 3.5.1 小节）。不过在代数系统中我们仍然坚持按人们习惯的方式来标识和使用运算符号，尤其是在二元运算的情况。例如，设 $\mathbf{Z}$ 是整数集合，两个整数 $i, j\in\mathbf{Z}$ 的加、减、乘、除运算，习惯上是以中**缀记法**这样表示的：$i+j$, $i-j$, $i\times j$, $i\div j$。要知道这四个运算符号实际上就是从 $\mathbf{Z}^2\rightarrow\mathbf{Z}$ 的函数符号，所以把它们写成 $+(i,j)$，$-(i,j)$，$\times(i,j)$，$\div(i,j)$ 也无不妥（它们被称为运算表达式的**前缀表达**方法），正如在写 $\mathbf{Z}^2\rightarrow\mathbf{Z}$ 的一个二元函数 f，将函数值记为 $f(i,j)$ 一样合理。

下面是一些运算的例子。

设 F 是在某区间 (a,b) 上有定义的全体可微分实函数，求导数就是 F 上的一个一元运算。

另外，大家熟悉的一元运算还有取实数的绝对值和相反数，等等。

必须事先说明，代数系统中所说的运算，已从我们原来理解的概念上大大推广了。再次强调，一个 n 元运算就是一个 n 元函数。致于用何种符号来标识一个运算不是本质的。在本章里，会出现大量的诸如“*”，“·”，“△”，“☆”等等运算符号。反正它仅仅是一种规则的代号，一个函数的符号。

下面来看一个日常生活中存在的代数系统，它描述了一台自动售饮料机的行为模式，如表 6.1 所示。

表 6.1　自动售饮料机

*	0	伍角硬币	一元硬币
0	无	橘子汁	矿泉水
伍角硬币	橘子汁	矿泉水	可乐
一元硬币	矿泉水	可乐	椰奶

自动售货机中有四种饮料：橘子汁、矿泉水、可乐和椰奶。售货机一次最多可接纳两枚硬币。若投入硬币的总值为 0.50 元时，机器给出一瓶橘子汁，投入 1.00 元时，给出一瓶矿泉水，投入 1.50 元时，给出一瓶可乐，投入 2.00 元时给出一瓶椰奶。实际上，自动售饮料机在执行一种二元运算“*”，它将一定值的硬币变换成某种饮料。设 $C=\{0$，伍角，壹元$\}$，二元运算 * 可用表 6.1 给出。其中 0 表示没有任何硬币投入。于是可以写出这样一些式子：伍角 * 伍角 = 矿泉水，壹元 * 0 = 矿泉水，0 * 0 =空（什么也不给）等等。像表 6.1 那样，完全描述某运算规则的表叫做运算的**复合表**。

从以上所举的种种例子可见，有一类运算所得结果（n 元函数的函数值）仍属于运算数所在集合（即 $X^n \to X$）。这种运算称为在 X 上是封闭的，如整数的加、减和乘运算。另一类运算所得结果不属于运算所在集合（即 $X^n \to Y$）。这种运算称为在 X 上是不封闭的，如以上自动售饮料机。

定义 6.2　设“*”是非空集 X 上的 n 元运算。若对于 $x_1, x_2, \cdots, x_n \in X$，$n$ 元运算的结果 $z = *(x_1, x_2, \cdots, x_n) \in X$，则称运算 * 在 X 上是**封闭的**。

定义 6.3　一个非空集 X，连同它上面定义的有限个封闭运算$\{f_1, f_2, \cdots, f_r\}$一道构成了一个代数系统，记为$<X, f_1, f_2, \cdots, f_r>$。

【例 6.1】　**Z** 是整数集。运算“·”是普通整数乘法。说明<**Z**,·>构成代数系统。

解　任取 $i, j \in \mathbf{Z}$，因为 $i \cdot j \in \mathbf{Z}$，所以乘法在整数集上是封闭的，于是<**Z**, ·>是一代数系统。

【例 6.2】　**R** 是实数集，运算“÷”是普通除法。说明 **R** 与÷不能构成代数系统。

解　因为 $0 \div 0$ 和 $r \div 0$ 均无意义，所以除法并非对实数中任意两个都是有定义的，所以 **R** 与÷不能构成代数系统。

【例 6.3】　设 A 是任意一个集合，$\rho(A)$ 是 A 的幂集。集合运算“∪”，“∩”，“～”是并、交、补运算。说明$<\rho(A), \cup, \cap, \sim, \phi, A>$是代数系统。

解　因为 $\rho(A)$ 上的任两个元素均是 A 的子集，它们的并、交、补运算的结果仍是 A 的子集[*]，其中前两个是二元运算，后一个是一元运算。另外平凡子集 ϕ，A 是两个零元运算。所有这些运算在 $\rho(A)$ 上是封闭的，故$<\rho(A), \cup, \cap, \sim, \phi, A>$构成代数系统。

[*] 我们在讨论集合 A 的所有子集的时候，总是假设全集是幂集 $\rho(A)$。这是自然的。

6.1.2 运算的性质

人们在对代数系统长期研究的过程中认识到，有一些代数系统有着某些特殊的性质，并且它们在理论上和应用方面都是十分重要的。现在开始，将逐一讨论这方面的内容。

让我们先来看看有哪些二元运算具有特殊性质。所以说这些性质是重要的，原因在于它们是客观世界中经常遇到的一些事物具有的行为的反映，同时也是进一步研究代数系统的基础。

定义 6.4 设“△”是代数系统$<X,\triangle>$上的二元运算，若对任意$x,y,z\in X$，均有$(z\triangle y)\triangle z=x\triangle(y\triangle z)$，则称运算△具有可**结合性**，或说△满足结合律。

例如，整数集 **Z** 和普通加法构成的代数系统$<\mathbf{Z},+>$，实数集 **R** 和普通乘法构成的代数系统$<\mathbf{R},\times>$，它们各自的运算都满足结合律。

定义 6.5 设“∘”是代数系统$<X,\circ>$上的二元运算。若对于$x,y\in X$，均有$x\circ y=y\circ x$，则称运算∘是可**交换的**，或者说运算∘满足交换律。

以上提到的普通加法和乘法都满足交换律。

定义 6.6 设 * 和△都是代数系统$<X,*,\triangle>$上的二元运算。若对$x,y,z\in X$，均有$(x*y)\triangle z=(x\triangle z)*(y\triangle z)$和 $x\triangle(y*z)=(x\triangle y)*(x\triangle z)$，则称二元运算△对于 * 是可分配的，也可以说运算△对于 * 满足分配律。

普通乘法对于加法是可分配的，但反过来，普通加法对乘法不满足分配律。

定义 6.7 设 “*”和“△”都是代数系统$<X,*,\triangle>$上的二元运算，两者都满足交换律。若对$x,y\in X$，总有$x*(x\triangle y)=x$和$x\triangle(x*y)=x$，则称**运算 * 连同△一起满足吸收律**。

【例 6.4】 在实数集 **R** 上定义以下两个二元运算 * 和△，对$r_1,r_2\in\mathbf{R}$，

$$r_1 * r_2=\max\{r_1,r_2\}$$
$$r_1\triangle r_2=\min\{r_1,r_2\}$$

验证 * 与△满足吸收律。

证明 * 与△都满足交换律自不成问题。另外，对于$r_1,r_2\in\mathbf{R}$，因为

$$r_1*(r_1\triangle r_2)=\max\{r_1,\min\{r_1,r_2\}\}=r_1$$
$$r_1\triangle(r_1*r_2)=\min\{r_1,\max\{r_1,r_2\}\}=r_1$$

证完。

定义 6.8 设“*”是代数系统$<X,*>$上的二元运算。若存在一个元素$x_l\in X$，使得对于任意$x\in X$都有$e_l*x=x$，则称e_l是关于运算 * 的左幺元；又若存在一个元素$e_r\in X$，对于任意$x\in X$都有$x*e_r=x$，则称e_r是关于运算 * 的右幺元；若存在一个元素$e\in X$，它既是左幺元也是右幺元，则称e是关于运算 * 的幺元。

表6.2给出了$X=\{a,b,c,d\}$上的两个二元运算 * 和△的复合表。从中可观察到关于 * 没有左幺元，有两个右幺元a和b；c是关于△的左幺元，而没有右幺元。

表 6.2

*	a	b	c	d
a	a	a	d	c
b	b	b	c	d
c	c	c	a	b
d	d	d	a	b

△	a	b	c	d
a	a	a	b	a
b	c	d	c	b
c	a	b	c	d
d	c	c	d	d

定理 6.1 设 “*” 是代数系统$<X,*>$上的二元运算，存在关于 * 的左、右幺元e_l，$e_r \in X$，则左幺元等于右幺元$e_l = e_r$，且有唯一幺元$e = e_l = e_r$。

证明 先证$e_l = e_r$。因为e_l是左幺元，e_r是右幺元，所以按定义有

$$e_r = e_l * e_r = e_l$$

令$e_l = e_r = e$，再证幺元e是唯一的。

反证法，若不然，还有$e_1 \in X$也是一个幺元，且$e_1 \neq e$，则有

$$e_1 = e_1 * e = e$$

矛盾。

定义 6.9 设 “*” 是代数系统$<X,*>$的二元运算，e是幺元。如果对于一个$x \in X$，存在一个$y \in X$，使$y * x = e$，则称y是x关于 * 的**左逆元**；如果对于一个$x \in X$，存在一个$y \in X$，使得$x * y = e$，则称y是x关于 * 的**右逆元**；若y同时是x的左逆元和右逆元，则称y是x的**逆元**。

应该指出，一个元素可以不存在左逆元或右逆元，也可以有多个左逆元或右逆元。

定理 6.2 设“*”是代数系统$<X,*>$的二元运算，* 满足结合律。e是幺元，若一个元素$x \in X$有左逆元y，也有右逆元z，则左逆元等于右逆元$y = z$，且这就是x的逆元。x的逆元记为x^{-1}，一个元素的逆元是唯一的。

证明 先证明左逆元y等于右逆元z。

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z$$

若x还有另一个逆元x_1^{-1}，则可类似以上定理 6.1 的证明方法证明$x_1^{-1} = x^{-1}$。

【例 6.5】 设集合$\mathbf{N}_k = \{0,1,2,\cdots,k-1\}$。代数系统$<\mathbf{N}_k,+_k>$定义二元运算$+_k$如下。对$x,y \in \mathbf{N}_k$，

$$x +_k y = (x + y)(\mathrm{mod}\, k)$$

试说明此代数系统的每一元素是否都有逆元。

解 显然，元素 0 是系统的幺元，此外，对任一个$x \in \mathbf{N}_k$，一方面$(k-x) \in \mathbf{N}_k$，同时还有

$$x +_k (k-x) = (k-x) +_k x = k(\mathrm{mod}\, k) = 0$$

所以，的确$\mathbf{N}_k$的每一元素均有唯一逆元。

定义 6.10 设“*”是代数系统$<X,*>$上的二元运算。若有$\theta_l \in X$，使一切$x \in X$都有$\theta_l * x = \theta_l$，则称θ_l是系统的一个**左零元**；又若有$\theta_r \in X$，使一切$x \in X$都有$x * \theta_r = \theta_r$，则称θ_r是系统的一个**右零元**；若$\theta \in X$同时是左零元和右零元，则称θ是系统的**零元**。

例如，实数构成的代数系统$<\mathbf{R},+,\times>$中，0 是关于加法的幺元，1 是关于乘法的幺元。每一个实数$r \in \mathbf{R}$有关于加法的逆元是$-r$；而每一个非零实数$r \neq 0$均有一个关于乘法的逆元$1/r$。此外在实数中不存在关于加法的零元，但存在关于乘法的零元，就是 0。

类似定理 6.1 可证以下关于零元的定理。

定理 6.3 如果代数系统$<X,*>$有左零元θ_l和右零元θ_r，则左零元等于右零元$\theta_l = \theta_r$，并且零元θ是唯一的：$\theta = \theta_l = \theta_r$。

6.2 半群和独异点

下面将讨论一些重要的代数系统的性质。让我们先从半群和独异点开始。

定义 6.11 设<X,*>是代数系统，若二元运算“*”满足结合律，则称此代数系统是一个**半群**。

定义 6.12 设<X,*>是代数系统，若二元运算“*”满足结合律，且系统含有幺元e，则此代数系统叫做**独异点**或**含幺半群**。

换言之，含有幺元e的半群，是独异点或含幺半群。

若幺元存在，对一个代数系统而言它是唯一的。所以独异点也可表示为一个由二元运算和一个零元运算（e）组成的代数系统<X,*,e>。

独异点有一个重要的性质，即独异点运算的复合表中不可能有两行或两列是相同的。证明是容易的，因为独异点含有唯一幺元。

【例 6.6】 设X是非空集。X^X表示一切X到X上的函数组成的集。又设运算“∘”表示X到X上函数的左复合。即，对于$f, g \in X^X$，复合函数$g \circ f$显然也是$X \to X$的函数，即$g \circ f \in X^X$。因此复合函数运算“∘”是在X^X上封闭的。按第 3 章 3.5.2 小节中定理 3.13，复合运算满足结合律，所以代数系统<X^X,∘>是半群。还有，X上的恒等函数I_X正是关于复合运算的幺元。因为$I_X \circ f = f \circ I_X = f$（参看第 3 章公式（3.63））。所以，我们有一个集合$X \to X$的所有函数的集合X^X上的独异点<X^X,∘, I_X>。

【例 6.7】 设A是任意确定的集合。可证明代数系统$<\rho(A), \bigcap, A>$是独异点。其中集合A就是关于交运算$\bigcap$的幺元。

因为任意集合$A_i, A_j \in \rho(A)$，它们的交集$A_i \bigcap A_j \in \rho(A)$。所以运算$\bigcap$是在$\rho(A)$上封闭的。

第 3 章 3.1.2 小节已表明，集合的交运算是可结合的。最后，对任意$A_k \in \rho(A)$，由幂集的定义可知，A_k是A的子集，$A_k \subseteq A$。故按第 3 章 3.1.2 小节交运算初等性质式(3.6)和式(3.11)，有$A_k \bigcap A = A \bigcap A_k = A_k$。所以集合$A$是关于交运算在幂集$\rho(A)$上的幺元。

这样就证明了$<\rho(A), \bigcap, A>$是独异点。

同样，可证明代数系统 $<\rho(A), \bigcup, \phi>$ 是独异点。空集ϕ是系统的幺元。

【例 6.8】 设Z是整数集合，$\mathbf{Z}_m$是由任意$m>1$的正整数为模的“模m同余”等价关系生成的等价类的集合（参考第 3 章 3.3.1 小节例 3.18 和例 3.19）。定义$\mathbf{Z}_m$上的两个二元运算“$+_m$”和“$\times_m$”如下。对于等价类$[i], [j] \in Z_m$

$$[i] +_m [j] = [(i + j) (\mathrm{mod}\, m)]$$

$$[i] \times_m [j] = [(i \times j) (\mathrm{mod}\, m)]$$

其中“+”和“×”是普通整数运算。

设$m = 5$。表 6.3 给出了这两个运算的复合表。

表 6.3

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\times_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

可见，运算$+_5$和$\times_5$在$\mathbf{Z}_m$上都是封闭的。由它们各自的定义容易证明，$+_5$和$\times_5$运算都是可结合的（读者可试算一下），并且$[0] \in \mathbf{Z}_5$是关于$+_5$运算的幺元，$[1] \in \mathbf{Z}_5$是关于$\times_5$运算的幺元。因此$<\mathbf{Z}_5, +_5, [0]>$和$<\mathbf{Z}_5, \times_5, [1]>$都是独异点。顺便提一下，复合表中没有两行或两列是

相同的。

关于半群和独异点有以下定理：

定理 6.4 设<X,*>是半群，Y 是 X 的子集。若二元运算 * 在子集 Y 上也是封闭的，即对任何 $x,y\in Y$，有 $(x*y)\in Y$，则 $<Y,*>$ 也是一个半群。通常称之为半群<X,*>的子半群。

证明 只要证运算“*”对于代数系统 $<Y,*>$ 是可结合的即可。

实际上，任取 $x,y,z\in Y$，因为 $y\subseteq X$，有 $x,y,z\in x$，而 * 在 X 上是可结合的，所以 $(x*y)*z=x*(y*z)$ 成立。考虑到 * 在 Y 上是封闭的，故 $(x*y),(y*z)$ 必属于 Y，于是以上等式两边的最后结果也属于 Y。这样就证明了以上结合律的等式在 Y 上成立。

一个最简单的子半群的例子是：偶数的加法半群 $<\mathbf{E},+>$ 是整数的加法半群 $<\mathbf{Z},+>$ 的子半群。

定理 6.5 设<X,*>是一个独异点。若 $x\in X$ 有逆元 x^{-1}，则有

$$(x^{-1})^{-1}=x \tag{6.1}$$

又若 $x,\ y\in X$，且 x,y 均有逆元 x^{-1}，y^{-1}，则有

$$(x*y)^{-1}=y^{-1}*x^{-1} \tag{6.2}$$

证明 因为

$$x^{-1}*x=x^{-1}*x=e$$

其中，e 是系统的幺元。按照逆元的定义 x 也是 x^{-1} 的逆元，于是式（6.1）得证。

另外，由

$$\begin{aligned}(x*y)*(y^{-1}*x^{-1})&=x*(y*y^{-1})*x^{-1}\\&=(x*e)*x^{-1}\\&=x*x^{-1}\\&=e\end{aligned}$$

和

$$\begin{aligned}(y^{-1}*x^{-1})*(x*y)&=y^{-1}*(x^{-1}*x)*y\\&=(y^{-1}*e)*y\\&=y^{-1}*y\\&=e\end{aligned}$$

并按逆元的定义可知 $(x*y)$ 的逆元是 $y^{-1}*x^{-1}$，即式（6.2 ）成立。

值得提醒的是，以上证明用到了“*”运算是可结合的（因为 $<X,*>$ 是独异点），否则不能得出要证的结论。

6.3 群和子群

群论是近世代数中的一个重要分支，在计算机科学领域中，群论有着重要的应用。

6.3.1 群的概念

定义 6.13 设 $<G,*>$ 是一个代数系统，二元运算 * 满足以下性质：

1．可结合性。

2．系统有关于“*”的幺元 e。

3．G 中任意元素 $x\in G$ 均有逆元 x^{-1}。

可见群实际上是一个其上任一元素都有逆元的独异点，或者说是含有幺元和每一元素均可逆的半群。

【例 6.9】 设 $X=\{1,2,3,4\}$，X 上的函数 f 如下给出

$$f=\{<1,2>,<2,3>,<3,4>,<4,1>\}$$

又设 $f^{(0)}$ 是 X 上的恒等函数 I_x。记各复合函数为：$f\circ f=f^{(2)}$，$f^{(2)}\circ f=f\circ f^{(2)}=f^{(3)}$，$f^{(3)}\circ f=f\circ f^{(3)}=f^{(4)}$。通过实际运算我们可知 $f^{(4)}=f^{(0)}$。以 $f^{(1)}$ 标识 f，有函数的集合 $F=\{f^{(0)},f^{(1)},f^{(2)},f^{(3)}\}$。表 6.4 给出了 F 上函数复合运算的复合表。从复合表中可以看出，函数复合运算“∘”在 F 上是封闭的，并由复合函数理论，运算“∘”满足结合律。表 6.4 显示了恒等函数 $f^{(0)}$ 是幺元，且每一函数 $f^{(i)}(i=1,2,3)$ 的逆元是 $f^{(4-i)}$，而 $f^{(0)}$ 的逆元就是它自己。

表 6.4

0	$f^{(0)}$	$f^{(1)}$	$f^{(2)}$	$f^{(3)}$
$f^{(0)}$	$f^{(0)}$	$f^{(1)}$	$f^{(2)}$	$f^{(3)}$
$f^{(1)}$	$f^{(1)}$	$f^{(2)}$	$f^{(3)}$	$f^{(0)}$
$f^{(2)}$	$f^{(2)}$	$f^{(3)}$	$f^{(0)}$	$f^{(1)}$
$f^{(3)}$	$f^{(3)}$	$f^{(0)}$	$f^{(1)}$	$f^{(2)}$

因此，代数系统 $<F,\circ>$ 是一个群。

还要指出的是，以上复合表中不仅没有两行或两列是相同的，而且每一行或列中的所有元素也各不相等。更明白地说，其每一行或每一列都是 F 中元素的一个全排列。这个重要的性质是每一群都有的本质属性。

定义 6.14 设 $<G,*>$ 是一个群。若 G 是有限集合，则 G 是**有限群**。

以记号 $|G|$ 表示集合中元素的数目，并称群 G 是 $|G|$ 阶的。

一个群若不是有限群，就称为**无限群**。

定理 6.6 群不含有零元。

证明 一阶群 $<\{e\},*>$ 中的元素 e 约定是幺元。

设 $|G|>1$。若 e 是幺元，并另有一个零元 $\theta\neq e$。则对任意 $x\in G$，按零元的定义有

$$x*\theta=\theta*x=\theta\neq e$$

这说明 $\theta\in G$ 是一个没有逆元的元素，与 G 是群矛盾。

定理 6.7 设 $<G,*>$ 是一个群。对于任意取定的 $a,b\in G$，方程 $a*x=b$ 有唯一解。

证明 $x=a^{-1}*b$ 是方程的一个解。因为

$$\begin{aligned}a*(a^{-1}*b)&=(a*a^{-1})*b\\&=e*b\\&=b\end{aligned}$$

再若还有一个不等于 x 的元素 x_1 也是方程的解，证明这将引出矛盾。因为 $a*x_1=b$，所以

$$a^{-1}*(a*x_1)=a^{-1}*b$$

$$(a^{-1}*a)*x_1=a^{-1}*b$$

$$e*x_1 = a^{-1}*b$$
$$x_1 = a^{-1}*b = x$$

矛盾。

定理 6.8 （可约律）设$<G,*>$是一个群。若对于$a,b,c\in G$，有$a*c=b*c$或者$c*a=c*b$，则$a=b$成立。

证明是简单的，请读者自己写出，并细细回味以上在证明各定理的时候，每一步推演过程都用到群的什么性质。如果觉得像可约律这样的结果是“自然可以约的”话，就得特别问一下自己为什么？问一问在半群和独异点中为什么没有可约律？即使在代数中，由$a\times c=b\times c$也是不一定可得到$a=b$的。不是吗？

还有一点要特别指出的是，即使在一般的群中，从等式$a*c=c*b$也是不可能推得$a=b$的。

定理 6.9 设$<G,*>$是一个有限群。则G的复合表中的每一行和每一列都是G的全部元素的全排列之一。

证明 分析可知，定理的结论实际上指出了群的每一个元素$x\in G$在复合表的每一行和每一列恰好出现一次。

先证明任一个$x\in G$，必在每一行中出现。不妨考察复合表中与元素$a\in G$对应的行。令$b=a^{-1}*x$，因为$a*b=a*(a^{-1}*x)=x$，所以x出现在与a对应的一行和与b对应的一列上。

再次证明以上元素x在与a对应的行上只有一个。实际上，若不然，在此行中x不仅出现在与b对应的列中，还出现在另一元素$c\in G$对应的列上，则有$a*b=x$和$a*c=x$，也即$a*b=a*c$。由可约律得$b=c$。矛盾。

同理可证结论对列也成立。

定义 6.15 代数系统<X,*>中，若存在元素$x\in X$，使$x*x=x$，则元素x叫**幂等元**。

独异点和群至少有一个幂等元是e。

定理 6.10 一个群不含除幺元之外的幂等元。

证明 设$<G,*>$是群，e是幺元。若$|G|=1$，则约定此唯一元素是幺元。

设$|G|>1$。若还有$x\in G$，$x\neq e$也是幂等元。则

$$x = x*x = x*e$$

利用可约律在上述第二个等式中约去x，则得$x=e$。矛盾。

显然，任何一阶群都是同构的（稍后，我们会严格定义群同构的概念。目前我们只要这样来理解群同构：将其中一个群的运算名和每一个元素适当地一一对应地置换成另一个群的运算名和元素之后，得到另一群的复合表）。

表 6.5 给出了二阶群的复合表。所有二阶群是同构的。表 6.6 给出了三阶群的复合表。

表 6.5

*	e	a
e	e	a
a	a	e

表 6.6

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

任何三阶群都是同构的。以上三种群的复合表均可根据幺元的性质和定理 6.9 与定理 6.10 直接写出来，并且其中每一种群在满足上述诸性质的情况下，复合表是唯一的。相信读者通过自己构造一个三阶群，会更深入地理解群的初等性质。

四阶群就复杂一些了。先前给出了一个是循环群的四阶群，表 6.4 是它的复合表。但并非所有四阶群都是同构于此循环四阶群的。表 6.7 给出了另一类四阶群的复合表，这就是所谓的克莱茵（Klein）四阶群。

表 6.7

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

【例 6.10】 验证表 6.7 给出的代数系统 $<K,*>$ 是一个群，其中 $K=\{e,a,b,c\}$。

证明 从复合表 6.7 可知，运算 * 在集合 $\{e,a,b,c\}$ 上是封闭的。考查它的第 1 行与第 1 列可知，e 是幺元。并且，因为 $a*a=b*b=c*c=e$，所以每一元素的逆元是它们自己。

最后，可证明运算 * 满足可结合律。在结合律的等式中，若三个元素中至少有一个是幺元，如 $(a*e)*b=a*(e*b)$ 等等，结论是显见的。对于其余含有 a,b,c 三元素的 $3^3=27$ 种等式（如 $(a*b)*b=a*(b*b)$ 等等），只要有耐心，也可一一证明之。

最后我们指出，任何四阶群必与循环四阶群或克莱茵群之一同构。

6.3.2 子群的概念

定义 6.16 $<G,*>$ 是一个群。对于 G 的一个非空子集 $S\subseteq G$，若 $<S,*>$ 也是一个群，就称之为是 G 的**子群**。

显然，$<\{e\},*>$ 和 $<G,*>$ 是 G 的子群，其中 e 是群上的幺元，并称这两个子群是 G 的**平凡子群**。若还有其他 G 的真子集连同二元运算 * 也是 G 的子群，把这些子群叫做是**非平凡子群**。

同一个群的每一子群都有一个幺元，问题是所有这些幺元是否都一样？又子群的幺元和原来衍生出这些子群的群的幺元是否相同呢？下面的定理给出了答案。

定理 6.11 一个群的幺元也是它每一个子群的幺元。

证明 设 $<S,*>$ 是群 $<G,*>$ 的子群。e' 和 e 分别是它们各自的幺元。要证 $e'=e$。

实际上，因为 e' 是 S 的幺元，所以 $e'=e'*e'$。又因为 $e'\in S$，而 $S\subseteq G$，所以 $e'\in G$。于是又有 $e'=e'*e$。即得

$$e'*e'=e'*e$$

在群 G 上利用可约律，消去等式两边的 e' 即得 $e'=e$。

在给出下面判断子群的定理之前，让我们先来约定一些记号。

约定群的一个元素 a 的正整次幂 $a^k(k\in Z^+)$ 的含义。首先

$$(\cdots((a_1*a_2)*a_3)\cdots*a_k) \tag{6.3}$$

是任意 k 个元素 $a_1,a_2,\cdots,a_k$ 按自左至右结合的运算结果。由于群上的运算满足结合律，所以，用归纳法可证，k 个元素按任意次序结合运算的结果与式（6.3）的结果是一致的。因此，可写出

$$a^k=\underbrace{a*a*\cdots*a}_{k个} \tag{6.4}$$

定理 6.12　设$<G,*>$是一个群，$S\subseteq G$是非空的有限子集。若运算 * 在S上是封闭的，那么$<S,*>$是$<G,*>$的子群。

证明　按假设“*”在S上是封闭，所以运算 * 在S上继承了它在群G中具有的结合律（参考定理 6.4 的证明）。

任取一元素$b\in S$，因 * 运算是封闭的，且S是有限集合，所以必有正整数i,j，且$i\neq j$，使

$$b^i=b^j$$

不妨设$i<j$。于是

$$b^i=b^i*b^{(j-i)}$$

可见$b^{(j-i)}$是G的幺元。

若$j-i=1$，就是说$b^i=b^i*b$，显然b就是G的幺元$b=e$，并且b的逆元就是自己：$b^{-1}=e^{-1}=e=b$。

若$j-i>1$，就有$b^{j-i}=b*b^{(j-i-1)}$。因为$b^{(j-i)}$是G的幺元，所以b的逆元$b^{-1}=b^{(j-i-1)}$。

至次，已证明$<S,*>$满足群的所有性质。

定理 6.13　设$<G,*>$是群，S是G的非空子集$S\subseteq G$。若对于$a,b\in S$，有$a*b^{-1}\in S$，则$<S,*>$是G的子群[*]。

证明　首先来证G的幺元e也属于S。取$a\in S$，按定理的前提有$a*a^{-1}=e\in S$。

其次来证对任意$a\in S$，a在群G上的逆元a^{-1}也属于S。因为已证$e\in S$，可以按假设$e*a^{-1}=a^{-1}\in S$。

再证 * 运算在S上封闭。事实上，任取$a,b\in S$，上面已证$b^{-1}\in S$，所以由假设有$a*(b^{-1})^{-1}=a*b\in S$。

最后由于已证运算 * 在S上封闭，所以它自然也继承了运算在群G中的可结合性。至此，我们已证明了S具有群的全部性质。

【例 6.11】　证明若$<G,*>$，$<H,*>$都是群$<X,*>$的子群，则$<G\bigcap H,*>$也是X的子群。

证明　任取$a,b\in G\bigcap H$，就是说$a,b\in G$和$a,b\in H$。因为G,H都是群，所以$b^{-1}\in G$和$b^{-1}\in H$。于是$a*b^{-1}\in G$和$a*b^{-1}\in H$，即$a*b^{-1}\in G\bigcap H$。最后按定理 6.13 直接可知$<G\bigcap H,*>$是G的子群，是H的子群，当然也是X的子群。

注意，定理 6.13 并不像定理 6.12 那样仅在有限子集上成立。

6.4　阿贝尔群和循环群

6.4.1　阿贝尔群

定义 6.17　若群$<G,*>$的二元运算 * 满足交换律，即$x,y\in G$，有$x*y=y*x$，则称G是**交换群**。交换群也叫**阿贝尔（Abel）群**。

在上一节中，例 6.9 和例 6.10 给出的两个四阶群都是阿贝尔群（它们的复合表是关于主对角线对称的）。事实上，任何不超过五阶的群都是阿贝尔群。

我们已在上一节中定义了$a^k(k>0,k$是正整数，$a\in G)$。现在再来约定

[*] 注意，本定理并不要求$b^{-1}\in S$。

$$a^0 = e \quad (e\text{是幺元}) \tag{6.5}$$

$$a^{-m} = \underbrace{a^{-1} * a^{-1} * \cdots * a^{-1}}_{m\text{个}} \quad (a^{-1}\text{是}a\text{的逆元}) \tag{6.6}$$

这样当n为任何整数，在群上幂a^n均有意义，并且可知，a^m的逆元就是a^{-m}

$$(a^m)^{-1} = a^{-m} \tag{6.7}$$

由此，可证明以下公式成立

$$a^m * a^n = a^{m+n} \tag{6.8}$$

$$(a^m)^n = a^{mn} \tag{6.9}$$

特别在交换群上，还有一个公式

$$(a*b)^m = a^m * b^n \tag{6.10}$$

在非零实数的普通乘法群$<R-\{0\},\times>$上，以上式（6.4）至式（6.10）诸公式是我们早就在代数中熟悉的幂运算的规律。这并不奇怪，因为以上普通乘法群只是交换群的一个特例。

容易明白，一个群$<G,*>$上的二元运算 * 用什么符号表示，或者为这个运算起一个什么名字并不重要，本质上重要的是这个运算必须满足群有关运算的所有性质。这样，如果将群$<G,*>$中的运算“*”用符号“+”来表示，只要后者与“*”有一样的运算复合表，并且满足群上有关运算的所有性质，那么群$<G,+>$与$<G,*>$就没有什么两样。这时，如我们称运算“+”为“加法”，那么按代数中习惯，我们可以将上式（6.4）至式（6.10）诸公式重写一遍，对于$a \in G$有

$$ka = \underbrace{a + a + \cdots + a}_{k\text{个}} \quad (k > 0) \tag{6.11}$$

$$0a = e \quad (e\text{是幺元}) \tag{6.12}$$

$$-ma = \underbrace{(-a) + (-a) + \cdots + (-a)}_{m\text{个}} \quad (m > 0) \tag{6.13}$$

$$-(ma) = -ma \tag{6.14}$$

$$(m+n)a = ma + na \tag{6.15}$$

$$m(na) = mna \tag{6.16}$$

另外，若$<G,+>$还是一个交换群的话，下面这个公式也成立

$$m(a+b) = ma + mb \tag{6.17}$$

应当指出，上式（6.4）至式（6.10）和式（6.11）至式（6.17）两组公式本质上是完全一致的，只是采用了不同的记法而已。

【例 6.12】 设$<G,*>$是群。若对每一个$a \in G$，有$a^{-1} = a$，则该群是阿贝尔群。

证明 显然，群必是独异点。利用上节定理 6.5 中第二个结果，对于$a,b \in G$，有

$$\begin{aligned} a*b &= a^{-1} * b^{-1} \\ &= (b*a)^{-1} \\ &= b*a \end{aligned}$$

【例 6.13】 证明一个群$<G,*>$是阿贝尔群的充要条件是：对于$a,b \in G$，有

$$(a*b)*(a*b) = (a*a)*(b*b) \tag{6.18}$$

证明 先证必要性。设$<G,*>$是阿贝尔群。则

$$\begin{aligned} (a*b)*(a*b) &= a*(b*a)*b \\ &= a*(a*b)*b \\ &= (a*a)*(b*b) \end{aligned}$$

再证充分性。设式（6.18）对 $a,b\in G$ 成立。于是

$$a*(b*a)*b=a*(a*b)*b$$

利用群的可约律依次消去等号中两式左右两端的 a 和 b 就有

$$b*a=a*b$$

6.4.2 循环群

回到本章 6.2 节例 6.8 给出的代数系统 $<\mathbf{Z}_5,+_5>$。容易证明这是一个群。现在来考查其元素（等价类）[2]的各累加和（这里，我们引用“加法”的习惯记法）：

$$1[2]=[2]，2[2]=[2]+_5[2]=[4]$$

$$3[2]=[1]，4[2]=[3]，5[2]=[0]，\cdots$$

我们发现，通过某个元素的不断“累加”的运算，就可以得到群上的所有元素。这种群叫做**循环群**。

定义 6.18 设 a 是群 $<G,*>$ 的一个元素 $a\in G$，若群上每一个元素 $b\in G$，均可表示成 a 的幂 $b=a^k$（或者说成 a 的累加和 ka），则称 G 是一个循环群，而元素 a 叫该循环群的一个**生成元**，并称群 G 可以由元素 a 生成。

现在可以说 $<\mathbf{Z}_5,+_5>$ 是循环群。元素[2]是一个生成元，并且除幺元[0]之外，$\mathbf{Z}_5$ 上每一元素都是生成元。经过仔细观察表 6.5 和表 6.6 我们还发现，所有不高于 3 阶的群都是循环群，而一切与 6.3 节例 6.9 同构的四阶群都是循环群。而克莱茵群不是循环群。那么更高阶的群是否会是循环群呢？或者说，几阶的群一定是循环群呢？这个问题是有解的，将在稍后讨论。

循环群的一个明显的特征就是它的复合表是关于主对角线对称的。事实上，一切循环群都是交换群。

定理 6.14 循环群都是交换群。

证明 设 $<G,*>$ 是循环群，$a\in G$ 是它的生成元。任意 $x,y\in G$，按循环群定义，x,y 可表示成 a 的幂的形式：$x=a^m$，$y=a^n$。于是

$$\begin{aligned}x*y&=a^m*a^n\\&=a^{m+n}\\&=a^{n+m}\\&=a^n*a^m\\&=y*x\end{aligned}$$

定义 6.19 设 $<G,*>$ 是群。e 是幺元，元素 $a\in G$。若存在整数 k，是使 $a^k=e$ 成立的最小正整数，则称 a 的阶（或周期）是 k，否则 a 的阶为 ∞。

定理 6.15 设 $<G,*>$ 是有限群，$a\in G$，且 a 的阶是 m，则集合

$$H=\{a,a^2,\cdots,a^m=e\}$$

连同运算 * 构成 G 的一个子群 $<H,*>$，其中 e 是 G 的幺元。

证明 先证明 H 上没有两个元素是相同的。若不然，有正整数 i,j（$1\leqslant i\leqslant m,1\leqslant j\leqslant m$），不妨设 $i<j$，使 $a^i=a^j$，那么 $a^i=a^i*a^{(j-i)}$，就是说 $a^{(j-i)}$ 是幺元：$a^{j-i}=e$，显然 $j-i<m$，这样 a 的阶是 $j-i<m$，与假设矛盾。

再来证 $<H,*>$ 是 G 的子群。应用 6.3 节定理 6.12，对 $a^p,a^q\in H$（$p\leqslant m,q\leqslant m,p,q$ 是正整数），只要证明 $a^p*a^q\in H$ 即可。

实际上，设 $p+q=m\cdot l+r$（l,r 是正整数，且 $0\leqslant r<m$）

$$a^p * a^q = a^{(p+q)} = a^{(ml+r)} = a^{ml} * a^r = (a^m)^l * a^r = e^l * a^r = e * a^r = a^r$$

而 $a^r \in H$ 。

显然，以上元素 $a\in G$ 生成了一个 G 的 m 阶子群，并且该子群是循环群。通常称这样生成的子群为**循环子群**。

6.5 置换群和伯恩赛德定理

6.5.1 置换群

定义 6.20 有限非空集合 S 到它自己的一个双射函数 $f:S\to S$ 叫做 S 的一个**置换**。当 $|S|=n$，就称 f 是一个 ***n* 元置换**。

集合 S 的所有置换的集合记为 S_n。因为在 S 的每一置换下像的集合对应一个由 S 上所有元素的全排列，而这样的全排列共有 $n!$ 个，所以 $|S_n|=n!$。

可以用一种直观的方法来表示 S 的每一个置换。我们将 S 中的元素写在一行上，而在紧接着的下一行上，写上相应上一行每一元素在置换下的像。习惯上一个置换用记号 σ_i 表示。例如 $S=\{a,b,c\}$，那么 S 的所有三元置换列出如下

$$\sigma_e=\begin{pmatrix}a & b & c\\ a & b & c\end{pmatrix}\quad \sigma_1=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix}\quad \sigma_2=\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix}$$

$$\sigma_3=\begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix}\quad \sigma_4=\begin{pmatrix}a & b & c\\ c & a & b\end{pmatrix}\quad \sigma_5=\begin{pmatrix}a & b & c\\ c & b & a\end{pmatrix}$$

显然，置换作为一种双射，它具有双射函数普遍具有的性质。例如，$\sigma_1,\sigma_2,\sigma_3\in S_n$。则 σ_1 的逆函数 σ_1^{-1} 也是一个置换，$\sigma_1^{-1}\in S_n$。左复合 $\sigma_1\circ\sigma_2$ 是置换，$\sigma_1\circ\sigma_2\in S_n$，并且复合运算。满足结合律：

$$(\sigma_1\circ\sigma_2)\circ\sigma_3=\sigma_1\circ(\sigma_2\circ\sigma_3)$$

我们还将恒等函数 I_s 记为 σ_e。当然，σ_e 是代数系统 $<S_n,\circ>$ 的幺元。

因此，有以下定理：

定理 6.16 设 S 是非空有限集。S_n 是所有 S 的置换的集合，“$\circ$”是置换的左复合运算。则 $<S_n,\circ>$ 是一个群，通常称它为集合 S 的**对称群**。

定义 6.21 对称群 $<S_n,\circ>$ 的子群叫做 S 的置换群。

以下是一个 $S=\{a,b,c,d\}$ 的四元置换群。

【例 6.14】 设 $S=\{a,b,c,d\}$，$G=\{\sigma_e,\sigma_1,\sigma_2,\sigma_3\}$，其中每一置换定义如下：

$$\sigma_e=\begin{pmatrix}a & b & c & d\\ a & b & c & d\end{pmatrix}\quad \sigma_1=\begin{pmatrix}a & b & c & d\\ b & a & c & d\end{pmatrix}$$

$$\sigma_2=\begin{pmatrix}a & b & c & d\\ a & b & d & c\end{pmatrix}\quad \sigma_3=\begin{pmatrix}a & b & c & d\\ b & a & d & c\end{pmatrix}$$

验证 $<G,\circ>$ 是置换群。

解 由本章 6.3 节定理 6.12 可知，只需以上任意两个置换的左复合结果仍然属于 G，即左复合在 G 上是封闭的。这需要逐一验证 9 种不含 σ_e 的两个置换复合的结果（含有幺元 σ_e 的结果是显然的）。

在这里，我们给出了两种情况的结果。写出 σ_1,σ_2 的关系矩阵

$$A_1=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\qquad A_2=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

于是可算出 $\sigma_2\circ\sigma_1$ 的矩阵 A_{12} 和 $\sigma_1\circ\sigma_2$ 的矩阵 A_{21}*

$$A_{12}=A_1\circ A_2=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\qquad A_{21}=A_2\circ A_1=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

从中可写出置换的复合

$$\sigma_2\circ\sigma_1=\begin{pmatrix}a&b&c&d\\b&a&d&c\end{pmatrix}=\sigma_3\qquad\sigma_1\circ\sigma_2=\sigma_3$$

定义 6.22 设 σ 是集合 S 的置换，若存在元素 $a_1,a_2,\cdots,a_r\in S$，使得 $\sigma(a_1)=a_2,\ \sigma(a_2)=a_3,\cdots,\sigma(a_r)=\sigma(a_1)$，且 S 的其他元素在置换 σ 下的像与原像相等，则称置换 σ 是一个**轮换**。记为

$$\sigma=(a_1\ a_2a_3\cdots a_r)$$

容易懂得，以上轮换也可等价地写成为

$$\sigma=(a_ia_{i+1}a_{i+2}\cdots a_ra_1a_2\cdots a_{i-1})$$

定义 6.23 设 $\sigma=(a_1a_2\cdots a_r),\ \tau=(b_1b_2\cdots b_s)$ 是集合 S 的两个轮换。如果 $\{a_1,a_2,\cdots,a_r\}\bigcap\{b_1,b_2,\cdots,b_s\}=\phi$，则称 σ 和 τ 是不相杂的。

定理 6.17 集合 S 的两个不相杂轮换的复合运算是可交换的。

证明 设 $\sigma=(a_1a_2\cdots a_r),\tau=(b_1b_2\cdots b_s)$ 是不相杂的轮换。令 $A=\{a_1,a_2,\cdots,a_r\},\ B=\{b_1,b_2,\cdots,b_s\}$。任取 $x\in S$，若 $x\in A$，则 $x\notin B$。那么

$$\tau\circ\sigma(x)=\tau(\sigma(x))=\sigma(x)\qquad(\because\sigma(x)\notin B)$$
$$\sigma\circ\tau(x)=\sigma(\tau(x))=\sigma(x)\qquad(\because x\notin B,\therefore\tau(x)=x)$$

故 $\tau\circ\sigma=\sigma\circ\tau$。类似可证 $x\in B$ 时结论也成立。

又若 $x\notin A$ 且 $x\notin B$，于是 $\sigma(x)=x,\tau(x)=x$，所以仍有

$$\tau\circ\sigma(x)=\tau(\sigma(x))=\tau(x)=x$$
$$\sigma\circ\tau(x)=\sigma(\tau(x))=\sigma(x)=x$$

仍得 $\tau\circ\sigma=\sigma\circ\tau$。

定理 6.18 集合 S 上的置换 σ 可以唯一地分解成若干不相杂轮换的复合。

在这里，我们只提供一个例子来说明此定理的证明线索。

【例 6.15】 设 $S=\{1,2,3,4,5,6,7\}$，置换

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\3&4&5&2&7&6&1\end{pmatrix}$$

试将 σ 分解成若干不相杂轮换的复合。

解 从 S 上任一元素开始相继求像，直至像轮回变为最初元素为止。不妨取元素 1，于是 $\sigma(1)=3,\sigma(3)=5,\sigma(5)=7,\sigma(7)=1$。得到第一个轮换 $\tau_1=$（1 3 5 7）。再从一个并不出现在

---

* 注意，这里和以下的讨论中，沿袭了函数的左复合记法，即“自右向左”复合。这决定了求置换复合时两矩阵的先后秩序。

已求出的轮换中的元素，如元素 2，继续类似地操作，$\sigma(2)=4,\sigma(4)=2$，又得另一个轮换 $\tau_2=(2\ 4)$。最后只剩下元素 6，因 $\sigma(6)=6$，它在置换下不改变，当然也可写成轮换 $\tau_3=(6)$。最后得到

$$\sigma=\tau_1\circ\tau_2\circ\tau_3=(1\ 3\ 5\ 7)\circ(2\ 4)\circ(6)$$

或者

$$\sigma=(1\ 3\ 5\ 7)\circ(2\ 4)$$

定义 6.24 **一个轮换的长度**就是该轮换中包含元素的个数。长度为 2 的轮换又叫**对换**。

容易懂得，一个轮换$(a_1a_2\cdots a_r)$可以表示成若干对换的复合：

$$(a_1a_2\cdots a_r)=(a_1a_r)\circ(a_1a_{r-1})\circ\cdots\circ(a_1a_3)\circ(a_1\circ a_2) \tag{6.19}$$

【例 6.16】 设 $S=\{1,2,3\}$。将下列置换写成对换的复合

$$\sigma=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

解 $\sigma=(1\ 2)$=$(1\ 2)\circ(1\ 3)\circ(1\ 3)$=$(1\ 3)\circ(1\ 3)\circ(1\ 2)$

【例 6.17】 设 $S=\{1,2,3,4\}$。置换

$$\sigma=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\quad\tau=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$$

求 $\tau\circ\sigma$, $(\tau\circ\sigma)^{-1}$ 和 $\sigma\circ\tau$。

解 首先各自分解 σ 和 τ 为不相杂的轮换

$$\sigma=(1\ 2)$$
$$\tau=(1\ 2\ 3\ 4)$$

于是

$$\begin{aligned}\tau\circ\sigma&=(1\ 2\ 3\ 4)\circ(1\ 2)\\&=(1\ 4)\circ(1\ 3)\circ(1\ 2)\circ(1\ 2)\\&=(1\ 4)\circ(1\ 3)\\&=(1\ 3\ 4)\end{aligned}$$

$$\begin{aligned}(\tau\circ\sigma)^{-1}&=((1,4)\circ(1,3))^{-1}\\&=(1,3)^{-1}\circ(1,4)^{-1}\\&=(1\ 3)\circ(1\ 4)\quad(\because(1,3)^{-1}=(1,3),\ \ (1,4)^{-1}=(1,4))\\&=(1\ 4\ 3)\end{aligned}$$

$$\begin{aligned}\sigma\circ\tau&=(1\ 2)\circ(1\ 2\ 3\ 4)\\&=(1\ 2)\circ(2\ 3\ 4\ 1)\\&=(1\ 2)\circ(2\ 1)(2\ 4)\circ(2\ 3)\\&=(2\ 4)\circ(2\ 3)\\&=(2\ 3\ 4)\end{aligned}$$

或直观地表示成

$$\tau\circ\sigma=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}\qquad(\tau\circ\sigma)^{-1}=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\qquad\sigma\circ\tau=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$$

6.5.2 伯恩赛德定理

集合 S 的一个置换群 $<G,\circ>$ 中，一个元素 $a\in S$ 被置换成另一元素 $b\in S$ 是一种等价关系。

这就是说，

1．总有 G 的一个置换将 a 置换为它自己。

2．若有置换把 a 映射成 b，就一定也有一置换把 b 映射为 a。

3．若元素 a 被两个置换相继作用后，先后得到元素 b 和 c，那么一定有一个置换可将 a 直接置换成 c。

有时，我们需要知道一个等价关系诱导产生的所有等价类（参考第 3 章 3.3 节的内容）。可是当集合含有的元素数量较大时，通过等价关系来寻找等价类的尝试令人望而生畏，因为这样做的计算量相当大。下面将给出的定理提供了一个解决这类问题行之有效的方法。

让我们先给出一些定义。

设 S 是非空集，$<S_n,\circ>$ 是 S 上的对称群。又设 $<G,\circ>$ 是 S 的一个置换群。构造一个 S 上的二元关系：

$$R=\{<a,b>\,|\,a,b\in S,(\exists\tau)(\tau\in G\wedge\tau(a)=b)\} \tag{6.20}$$

现在来证明由式（6.20）定义的是一个等价关系。

定理 6.19　设 $<G,\circ>$ 是 S 的一个置换群，由式（6.20）定义的二元关系是等价关系。

证明　自反性。设 $a\in S$，因为单位置换（也即 G 的幺元）$\tau_e\in G$，且 $\tau_e(a)=a$。

对称性。设 $a,b\in S$，并且 $\tau\in G$，使得 $\tau(a)=b$。因为 τ 的逆置换 $\tau^{-1}\in G$，所以 $\tau^{-1}(b)=a$。

传递性。设 $a,b,c\in S$，并且 $\tau_1,\tau_2\in G$，使得 $\tau_1(a)=b,\tau_2(b)=c$。因为 $\tau_2\circ\tau_1\in G$（群上运算是封闭的），令 $\tau_2\circ\tau_1=\tau$，那么 $\tau(a)=\tau_2\circ\tau_1(a)=\tau_2(\tau_1(a))=\tau_2(b)=c$。

定义 6.25　a 是集合 S 中的元素，$a\in S$，若在 S 的一个置换 τ 下 a 并不改变，即 $\tau(a)=a$，则元素 a 叫做是置换 τ 下的一个**不变元**。

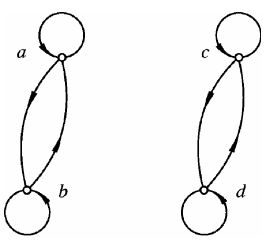


图 6.1　置换群诱导的等价关系

例如，在例 6.14 中，σ_e 有 a,b,c,d 四个不变元，σ_1 有两个不变元 c,d，σ_2 也有两个不变元是 a,b，而 σ_3 没有不变元。

我们称由式（6.20）定义的关系为置换群 G 诱导的等价关系，并且在图 6.1 给出了由例 6.14 的置换群诱导出的等价关系的关系图。

伯恩赛德（Burnside）定理告诉我们，一个由 S 的置换群 $<G,\circ>$ 诱导的等价关系，其等价类的数目等于 G 中每一置换的不变元数目之和（两个不同置换下相同的不变元重复计次）与群 G 的阶数 $|G|$ 之商。在这里提到的例子中，不变元数目是 $4+2+2+0=8$，群 G 是 4 阶的，因此等价类的数目是 $(4+2+2+0)/4=2$ 个。

定理 6.20　设 R 是非空集合 S 的置换群 $<G,\circ>$ 诱导的等价关系。R 的等价类的个数是

$$|S/R|=\frac{1}{|G|}\sum_{\tau\in G}\psi(\tau) \tag{6.21}$$

其中 $\psi(\tau)$ 表示置换 τ 的不变元个数。

证明　设 $x\in S$，用 $\eta(x)$ 记群 G 中那些以 x 为不变元的置换的数目。显然，对 S 中每一元素逐一求出 $\eta(x)$ 并相加 $\sum_{x\in S}\eta(x)$，其值一定等于 G 的每一置换下不变元数目之和 $\sum_{\tau\in G}\psi(\tau)$：

$$\sum_{x\in S}\eta(x)=\sum_{\tau\in G}\psi(\tau)$$

设 $x_0,x_i\in S$，且 x_0,x_i 同属一个等价类，即 x_0Rx_i（参考第 3 章定理 3.9）。不妨记这个等价类为 $[x_0]$。我们来证明 G 中恰有 $\eta(x_0)$ 个置换将 x_0 置换为 x_i。

事实上，因 $x_0 R x_i$，所以有一个置换 $\tau \in G$，使 $\tau(x_0) = x_i$。设 $A = \{\tau_1, \tau_2, \cdots\}$ 是含有不变元 x_0 的 $\eta(x_0)$ 个置换，且两两各不相同，那么集合 $B = \{\tau \cdot \tau_1, \tau \circ \tau_2, \cdots\}$ 就是将 x_0 置换成 x_i 的 $\eta(x_0)$ 个置换。这些置换两两各不相同。因为，若不然，有 $\tau \circ \tau_i = \tau \circ \tau_j$，那么按群的可约律得到 $\tau_i = \tau_j$，矛盾。

另外，可证明并不存在不属于集合 B 的置换 $\tau' \notin B$，且 $\tau'(x_0) = x_i$。因为若不然，以置换 τ 的逆 τ^{-1} 与之复合有 $\tau^{-1} \circ \tau'$，显然 $\tau^{-1} \circ \tau'$ 是一个以 x 为不变元的置换，于是 $\tau^{-1} \circ \tau' \in A$。但这是不可能的，因为果真如此，就有 $\tau \circ (\tau^{-1} \circ \tau') = \tau' \in B$。矛盾。

假设 $x_0, x_1, \cdots, x_i, \cdots, x_{k-1}$ 是同属等价类[x_0]的所有 k 个元素，现在对 G 的置换逐一地累加到以下各数值中去：x_0 映射为 x_0 的置换数目，x_0 映射为 x_1 的置换数目…，x_0 映射为 x_{k-1} 的置换个数，并求和。因为每一个 G 的置换必属于以上某一种情形（回忆公式（6.20）），还因为上面实际已证明每一类这种置换的数目都恰好是 $\eta(x_0)$ 个，所以

$$|G| = \eta(x_0) \cdot |[x_0]|$$

或者

$$\eta(x_0) = |G| / |[x_0]|$$

其中 $|[x_0]| = k$ 是等价类 $[x_0]$ 含有的元素个数。

同理，对等价类 $[x_0]$ 中其余每一元素也都是

$$\eta(x_1) = \eta(x_2) = \cdots = \eta(x_{k-1}) = |G| / |[x_0]|$$

因为，可以像推导 $\eta(x_0)$ 的值一样来得到它们。于是

$$\sum_{x_i \in [x_0]} \eta(x_i) = |G|$$

以上这个等式，对 S 的由置换群 G 诱导的每一个等价类都是正确的。所以

$$\sum_{x \in S} \eta(x) = \sum_{\tau \in G} \psi(\tau) = |S/R| \circ |G|$$

这样也就证得了等式（6.21）。

【例 6.18】 设 $S = \{a, b, c, d\}$，S 的三个置换如下

$$\tau_0 = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} \quad \tau_1 = \begin{pmatrix} a & b & c & d \\ b & c & a & d \end{pmatrix} \quad \tau_3 = \begin{pmatrix} a & b & c & d \\ c & a & b & d \end{pmatrix}$$

通过直接验证可知 $G = <\{\tau_0, \tau_1, \tau_2\}, \circ>$ 是置换群。试计算由以上置换群诱导的等价关系含有的等价类的数目。

解 计算每一置换的不变元的数目：

$$\sum_{\tau \in G} \psi(\tau) = 4 + 1 + 1 = 6$$

如今 $|G| = 3$，所以等价类的个数是 6/3= 2 个。观察可知，这两个等价类分别是 $\{a, b, c\}$ 和 $\{d\}$。

【例 6.19】 设有黄、蓝、白三色串珠，用它们串成 5 粒珠子的手镯。问可以有多少不同颜色组合的手镯？

解 两个手镯，其中之一在不翻面的情况下，通过旋转而成为与另一个一样的手镯，那么我们自然认为这两个手镯构造是无区别的（或称旋转等价的）。不考虑旋转等价的情况下，由 5 粒串珠共可串成 $3^5 = 243$ 只手镯。设它们组成集合 S。令 $G = \{\tau_0, \tau_1, \tau_2, \tau_3, \tau_4\}$，其中 τ_0 表示每一手镯不做旋转而对应它自己的置换，其他 τ_i（i=1,2,3,4），对应一只手镯按约定的方向——譬如，顺时针方向——旋转 i 粒珠子的位置而得到另一只手镯的置换。可以证明，$<G, \circ>$

是 S 上的一个置换群。因为接续两次旋转（置换的复合）的结果可以用一次旋转来代替。即旋转这种置换在 G 上是封闭的。事实上，$\tau_j \circ \tau_i$（连续转过 i 粒和 j 粒珠子）的效果，与一次转过 $k=(i+j)(\mathrm{mod}5)$ 粒珠子的置换 τ_k 的效果是一样的。对于对称群 $<S_{243},\circ>$ 来说，它包含了 243!个置换，除以上 G 所含有的 5 种旋转之外，全部都是不可用旋转实现的（例如纯白的手镯在旋转下绝不能映射成全蓝色的手镯—— 一个极端的例子）。因为 G 是 $<S_{243},\circ>$ 的一个有限子集，且旋转置换是封闭的，所以按本章定理 6.12 可知 $<G,\circ>$ 是一个置换群。

现在，只要求出由 G 诱导的等价类的数目便是不同串珠的数目。因为同一等价类的串珠总可以通过旋转从其中一个重合到另一个上去，且使两手镯重合的珠子是同色的。

按伯恩赛德定理，先求出 G 上不变元的个数：τ_0 有 243 个不变元，τ_1 有 3 个不变元，它们分别对应三种纯色的手镯。同样 τ_2,τ_3,τ_4 也各有 3 个这样的不变元。所以最后算出考虑旋转等价的情况下（即经旋转，如一个手镯与另一个完全相同的话，它们就是同一种手镯），有 $(243+3+3+3+3)/5=51$ 种不同的手镯。顺便说一下，如果还要考虑有些手镯翻一面就是另一些（即镜像对称）的情况，则就只有 39 种不同的手镯了。

实际上，我们在集合 $S'=$｛上述已求得的 51 种手镯｝上定义二种运算：T_0 和 T_1。它们分别对应不把手镯翻面和将手镯翻面一次。于是我们得到一个集合 S' 上的置换群：$<\{T_0,T_1\},\circ>$。它有 51 个对应 T_0 的不变元；有 3^3 个对应 T_1 的不变元（该种手镯对于通过某一粒串珠的轴是轴对称的，见图 6.2。像这样结构而串珠又不完全一样的图有 3^3 种，它们对应对称轴上的一粒和对称轴任意一边的两粒在一起的全排列的数目 3！种），所以最后这 51 个手镯在考虑翻面等价（一个翻一面是另一个的所有手镯只能被看成一个）的情况下，就只有 $\frac{(51+3^3)}{2}=39$ 种。

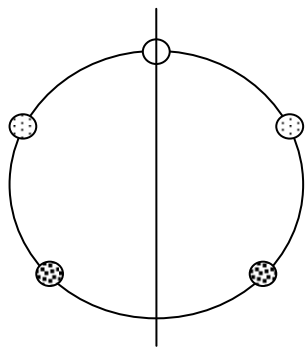


图 6.2　具有翻转等价性质的手镯

6.6　陪集和正规子群

陪集是一种集合的二元运算。陪集与下一节将要讨论的拉格朗日定理的证明有直接的关系。

定义 6.26　设 $<G,*>$ 是一个群，$A\subseteq G$，$B\subseteq G$。A,B 是两个非空的子集。记

$$AB=\{a*b|a\in A,b\in B\}$$

$$A^{-1}=\{a^{-1}|a\in A\}$$

并且称 AB 是 A 和 B（关于运算 * ）的积，称 A^{-1} 是集合 A（关于群 G ）的**逆**。

可以将两集合关于运算 * 的积推广到多于两个集合的情形。由于以上积的定义和群的运算是封闭和可结合的，可知 A,B,C 是 G 的非空子集，则 AB 和 BC 也是 G 的子集，并且有

$$(AB)C=A(BC) \qquad (6.22)$$

因此，我们可以无歧义地将三个集合 A,B,C 关于运算 * 的积简记成“ ABC ”。

特别当集合 $A=\{a\}$ 是一个元素组成的集合时，我们也常以“ aB ”的简化记法来代替 $\{a\}B$。

定义 6.27　设 $<H,*>$ 是群 $<G,*>$ 的子群。a 是 G 的一个元素 $a\in G$。积 $\{a\}H$ 就是由 a 确

定的 H 在群 G 上的一个**左陪集**，简称左陪集 *。记为 aH，即

$$aH=\{a*h|h\in H\}$$

类似地可以定义右陪集 Ha。

【例 6.20】 设 m 是一个正整数，$H=\{n\mid n=k\cdot m,k\in \mathbf{Z}\}$ 是所有整数的 m 倍组成的集合。容易验证 $<H,+>$ 是加法群 $<\mathbf{Z},+>$ 的一个子群。H 在 $\mathbf{Z}$ 上的左陪集共有 m 个，它们是

$$0H=\{\cdots,-2m,-m,0,m,2m,\cdots\}$$
$$1H=\{\cdots,-2m+1,-m+1,1,m+1,2m+1,\cdots\}$$
$$\cdots$$
$$(m-1)H=\{\cdots,-m-1,-1,m-1,2m-1,3m-1,\cdots\}$$

观察发现，以上 m 个陪集恰好就是整数集 $\mathbf{Z}$ 上的模 m 同余关系诱导的等价类（参阅第 3 章 3.3.1 小节的例 3.19）。

如果 $<G,*>$ 是阿贝尔群，则 H 的左、右陪集一定相等。若 G 不是阿贝尔群，则 H 的左、右陪集可能相等，也可能不等。

定义 6.28 设 $<H,*>$ 是 $<G,*>$ 的子群。H 是一个**正规子群**，当且仅当每一个 $a\in G$ 的元素确定的 H 的左陪集等于右陪集。即

$$aH=Ha$$

一个明显的事实是：阿贝尔群的每一子群都是正规子群。任何群的两个平凡子群都是正规子群。

值得特别指出的是，一般情况下即使 H 是 G 的正规子群，即 $aH=Ha$，但对于 $h\in H$，不必有 $a*h=h*a$。而可能是存在 H 的两个元素 $h_1,h_2\in H$，使得 $a*h_1=h_2*a$。

【例 6.21】 设 $S=\{1，2，3\}$，$<S_3,\circ>$ 是 S 的对称群。证明 $H=<\{I_s,\tau_1=(1\ 2)\circ(1\ 3),\ \tau_2=(1\ 3)\circ(1\ 2)\}$，$\circ>$是置换群，而且还是 S_3 的一个正规子群。其中 I_s 表示集合 S 上的恒等置换。

证明 验证 H 上的复合运算是封闭的。因为

$$I_s\circ I_s=I_s,\ I_s\circ\tau_1=\tau_1\circ I_s=\tau_1,\ I_s\circ\tau_2=\tau_2\circ I_s=\tau_2$$

还有

$$\tau_2\circ\tau_1=(1\ 3)\circ(1\ 2)\circ(1\ 2)\circ(1\ 3)=I_s$$
$$\tau_1\circ\tau_2=(1\ 2)\circ(1\ 3)\circ(1\ 3)\circ(1\ 2)=I_s$$
$$\tau_1^2=\tau_2,\ \tau_2^2=\tau_1$$

实际上，从运算是封闭的即可知 H 是群（定理 6.12）。

接下来证明 H 是正规子群。为此，做左陪集

$$(1\ 2)\circ I_s=(1\ 2)$$
$$(1\ 2)\circ\tau_1=(1\ 2)\circ((1\ 2)\circ(1\ 3))=(1\ 3)$$
$$(1\ 2)\circ\tau_2=(1\ 2)\circ((1\ 3)\circ(1\ 2))$$
$$=(1\ 2)\circ(1\ 2\ 3)$$
$$=(1\ 2)\circ(2\ 3\ 1)$$
$$=(1\ 2)\circ\ (2\ 1)\circ(2\ 3)$$
$$=(2\ 3)$$

* 有一些文献或教科书将 aH 叫做右陪集，而将 Ha 称为左陪集。

就是说，$(1,2)H=\{(1\ 2),(1\ 3),(2\ 3)\}$。

H 的另一个左陪集 $I_sH=H$ 。

最后，可以直接计算证实 H 的其他元素生成的左陪集都与以上两个左陪集之一相等。

因为 $S_3=\{I_s,(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(3\ 2\ 1)\}$，通过计算，可得

$$(1\ 3)H=(1\ 2)H \qquad (2\ 3)H=(1\ 2)H$$
$$(1\ 2\ 3)H=I_sH=H \qquad (3\ 2\ 1)H=H$$

要证明 H 是正规子群，还需逐一对以上各左陪集证明它们各自与相应的右陪集相等。下面的计算请读者作为练习来完成。

通过以上的证明，读者可能会对证明一个正规子群的计算量之大感到担忧。不过，这种疑虑在很大程度上是不必要的。除非我们要证明的是一个具体的正规子群，就如以上例题那样，否则，以下的定理在论证正规子群方面有着重要的理论价值。

定理 6.21 设 $<H,*>$ 是 $<G,*>$ 的子群。H 是正规子群的充要条件是对每一个 $g\in G$ 的元素，均有 $gHg^{-1}\subseteq H$ 成立。

证明 必要性。

设 H 是正规子群。任取 $g\in G$，由正规子群定义有 $gH=Hg$，于是 $(gH)g^{-1}=(Hg)g^{-1}$，因集合的积有结合律，所以 $gHg^{-1}=H(gg^{-1})=H$ 。当然也有 $gHg^{-1}\subseteq H$ 成立。

充分性。

设 $<H,*>$ 是 $<G,*>$ 的子群，并且对 $g\in G$ 有 $gHg^{-1}\subseteq H$ 。对于 $g^{-1}\in G$，就是 $g^{-1}H(g^{-1})^{-1}\subseteq H$，或 $g^{-1}Hg\subseteq H$，故 $g(g^{-1}Hg)g^{-1}\subseteq gHg^{-1}$，或者 $H\subseteq gHg^{-1}$，这样就得到 $gHg^{-1}=H$ 。

将以上最后一个等式两边各乘以 g，最后有

$$(gHg^{-1})g=gH=Hg$$

所以，H 是正规子群。

【例 6.22】 设 H_1,H_2 都是 G 的正规子群，证明 $H_1\bigcap H_2$ 也是 G 的正规子群。

证明 任取 $h\in H_1\bigcap H_2$，则 $h\in H_1,h\in H_2$。因为 H_1 和 H_2 是正规子群，所以按定理 6.21 的必要性可得，对任意一个 $g\in G$ 有 $g*h*g^{-1}\in H_1$ 和 $g*h*g^{-1}\in H_2$ 。也就是 $g*h*g^{-1}\in H_1\bigcap H_2$。由于 h 是 $H_1\bigcap H_2$ 的任意元素，所以 $g(H_1\bigcap H_2)g^{-1}\subseteq H_1\bigcap H_2$。最后根据定理 6.21 的充分性可得 $H_1\bigcap H_2$ 是 G 的正规子群的结论。

6.7 拉格朗日定理

我们已经看到，对一个群 $<G,*>$ 的子群 $<H,*>$，可以用一个属于群 G 的元素 $a\in G$ 生成左陪集和右陪集。从 6.6 节的例 6.21 可见，由两个不同元素生成的左（右）陪集可能是相同的，并且子群 H 本身也是一个左陪集 $eH=H$，是一个右陪集 $He=H$（其中 e 是幺元）。在 H 是有限群的情况下，人们会问：H 的不同左（右）陪集含有元素的数目是否是相同的？不同的左（右）陪集一共有多少个？下面的定理全面回答了这些问题。

定理 6.22 设 $<H,*>$ 是 $<G,*>$ 的有限子群。H 的每一个左陪集或右陪集包含有元素的个数等于 H 本身包含元素的个数。

证明 针对左陪集证明。右陪集的证明与此类似。

设 $H=\{h_1,h_2,\cdots,h_r\}$，即子群 H 共有 r 个不相同的元素，$a\in G$。任取 $h_i,h_j\in H$，且 $h_i\neq h_j, a*h_i\in aH, a*h_j\in aH$，但 $a*h_i\neq a*h_j$。因为若不然，$a*h_i=a*h_j$，利用群的可约律消去等式两边元素 a，得 $h_i=h_j$。矛盾。由此可知 $|aH|\geqslant|H|$。

另一方面，按左陪集定义，应该有 $|aH|\leqslant|H|$，结合上述证明的结果，所以 $|aH|=|H|$。

定理 6.23　（Lagrange 拉格朗日引理） $<H,*>$ 是 $<G,*>$ 的子群。G 上二元关系定义如下：

$$R=\{<x,y>\,|\,x\in G,y\in G,(\exists t)(t\in H\ \wedge\ x*t=y)\}$$

则 R 是一个等价关系，并且由 R 诱导的等价类与 H 的左陪集一一对应。

证明　设 e 是群 G 和 H 的幺元。

R 是自反的。因为任取 $x\in G$，令 $t=e$，就有 $x*e=x$，即 xRx。

R 是对称的。因为若 $x\in G,y\in G,xRy$。就是说，存在 $t\in H$，满足 $x*t=y$。那么由于 H 是一个子群，对元素 $t\in H$，有逆元 $t^{-1}\in H$。于是从等式 $x*t=y$ 可得 $y*t^{-1}=x$，所以 yRx。

R 是传递的。若 $x\in G,y\in G,z\in G$，且 xRy,yRz。即存在 $t\in H$ 和 $s\in H$，满足 $x*t=y$ 和 $y*s=z$。将以上两式联解就有 $(x*t)*s=z$，或者 $x*(t*s)=z$。显然，因为 $(t*s)\in H$，所以 xRz。

再来证引理的后一部分。

设 $a\in G$，以 a 为代表元素的等价类是 $[a]_R$。设 $x\in[a]_R$，根据等价类的定义可知，aRx。再由 R 的定义，存在 $h\in H$，满足 $a*h=x$，即 $x\in aH$，所以 $[a]_R\subseteq aH$。

又设 $x\in aH$，根据左陪集定义，存在 $h\in H$，使 $x=a*h$，所以 aRx，即 $x\in[a]_R$。于是，$aH\subseteq[a]_R$。结合刚才得到的结果 $[a]_R\subseteq aH$，故 $[a]_R=aH$。

定理 6.24　（Lagrange 拉格朗日定理） 有限群 G 的每一个子群的阶可以整除群 G 的阶。

证明　设 $|G|=n,\ |H|=m$。来证 $m|n$（n/m 是整数）。

因为每一个 G 的元素 $a\in G$ 一定属于一个左陪集，$a\in aH$。所以

$$G\subseteq\bigcup_{x\in G}xH$$

另外，按左陪集的定义和运算在群上封闭可知

$$\bigcup_{x\in G}xH\subseteq G$$

于是

$$\bigcup_{x\in G}xH=G$$

设 G 共有 q 个不同的左陪集，按以上定理 6.22，每一左陪集都含有 m 个元素，就是说 $n=q\cdot m$。证完。

推论 1　质数阶的群没有非平凡子群。

推论 2　质数阶的群一定是循环群。

证明　设群 $<G,*>$ 是质数阶的，$|G|=p\geqslant 2$，是一质数。任取一元素 $a\in G$，且 a 不是 G 的幺元。设元素 a 的阶是 m。即有子集

$$H=\{a,a^2,a^3,\cdots,a^m=e\}$$

根据本章定理 6.15 可知，H 是 G 的循环子群。按拉格朗日定理，m 整除 p。因 $a\neq e$，所以 $m\geqslant 2$。但 p 是质数，所以只能是 $m=p$。由 a 生成的循环子群正是 G 自己。

由此可得以下推论。

推论 3 质数阶群的任何一个非幺元元素的阶都等于该群的阶，且可由它生成这个质数阶群。

6.8 同态、同构和同余

6.8.1 同态和同构

本章的 6.3.1 小节中已在不严格的情况下提到过群的同构。本节将从代数系统出发，介绍同态和同构的概念。

定义 6.29 设$<G,*>$和$<S,\triangle>$是两个代数系统。若有一个映射 $f:G\to S$，使得任何 $x_1\in G,x_2\in G$，都有

$$f(x_1*x_2)=f(x_1)\triangle f(x_2) \tag{6.23}$$

成立。则称 f 是从代数系统$<G,*>$到$<S,\triangle>$的一个**同态映射**。而像集 $f(G)$ 称为**同态像**。

同态映射也简称为**同态**。

直观地可以这样来理解同态映射。即，在一个代数系统下两个元素 x_1,x_2 以及它们的运算结果 x_1*x_2 被 f 映射成另一代数系统上的像 $f(x_1),f(x_2)$ 以及 $f(x_1*x_2)$ 之后，这些像之间仍保持着运算关系（当然是关于像所在代数系统的运算来说的）。或者，也可以这样来诠释同态：一个代数系统中的两个元素 x_1,x_2，先运算得到一结果 x_1*x_2，再映射得到它的像 $f(x_1*x_2)$，和将它们先映射成像 $f(x_1),f(x_2)$，再在另一代数系统下求结果 $f(x_1)\triangle f(x_2)$。两次所得的结果总是相同的（结合图 6.3 来理解）。

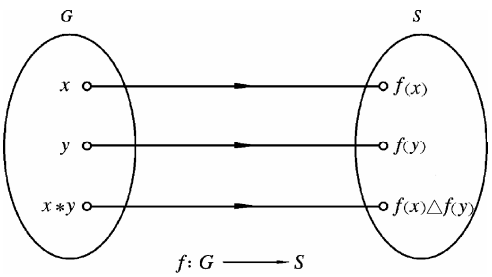


图 6.3 同态映射保持运算关系

引入同态的概念后，可将对一个代数系统的某些特征的研究，转换到一个相对较简单的另一个代数系统下来进行。下面是两个例子。

【例 6.23】 $<Z,+>$是整数加法群。另一个群由两个元素 **E**（偶数，Even）和 O（奇数，Odd）组成代数系统$<\{\mathbf{E},\mathbf{O}\},\oplus>$，并如表 6.8 那样定义运算。

表 6.8

⊕	**E**	**O**
E	**E**	**O**
O	**O**	**E**

求一个加法群到$<\{\mathbf{E},\mathbf{O}\},\oplus>$的同态映射。

解 首先，可方便地验证$<\{\mathbf{E},\mathbf{O}\},\oplus>$是一个群。我们要求一个群同态 f。

给 f 的定义如下：对 $i\in\mathbf{Z}$

$$f(i)=\begin{cases}\mathbf{E} & \text{当}i\text{是偶数}\\ \mathbf{O} & \text{当}i\text{是奇数}\end{cases}$$

现在来证，这样定义的映射 f 是同态映射。事实上，任取 $i,j\in\mathbf{Z}$，因为加法“+”和运算“$\oplus$”都是可交换的，可以只列举 3 种情况：（1）i 和 j 都是偶数，（2）i 和 j 都是奇数，（3）i 是奇数而 j 是偶数。显然，无论是哪一种情况，以下等式都是成立的

$$f(i+j)=f(i)\oplus f(j)$$

故而，f 是一个同态映射。

以上是一个关于同态的简单例子。但它的确简单明了地解释了引入同态的理由。譬如，要问 379 597 与 198 529 的和是奇数还是偶数这样的问题。读者大概不会先把这两个六位数加起来，然后再看这个和的奇偶性吧？一定会这样回答：“两个奇数之和一定是偶数。”恐怕连小学生都会这样做的。那么，读者是否想过呢？在读者这样思考问题的时候，难道不是在用我们以上给出的表 6.8 的结果吗？关于以上两个六位数之和的奇偶性问题，一种解决方法是先求出它们的和 379 597+198 529=578 126，然后确定它为偶数；而另一种解决方法是先确定这两个数都为奇数（映射为 **O**），然后用表 6.8 运算得知这两个数的和为偶数（**E**）。哪一种方法更简单是不用说的。可以说，同态并不是一个深奥的概念，很多时候人们在应用它，只不过是不自觉罢了。

下面是另一个稍稍复杂一些的关于同态的例子。

【例 6.24】 设$<\mathbf{Z},+>$是整数加法群。$<\mathbf{Z}_5,+_5>$是由“模 5 同余”诱导的等价类 $\mathbf{Z}_5=\{[0],[1],[2],[3],[4]\}$ 和运算“$+_5$”构成的代数系统。$+_5$ 运算已在本章 6.2 节表 6.3 左边的复合表定义。试构造一个同态映射 $f:\mathbf{Z}\to\mathbf{Z}_5$。

解 令 f 的定义如下

$$f(i)=[i(\mathrm{mod}5)]$$

可以证明，这样定义的映射是一个同态映射。

实际上，设 $i\in\mathbf{Z},j\in\mathbf{Z}$。令 $i=5\cdot p+r_1$（$p\in\mathbf{Z},0\leqslant r_1<5$），$j=5\cdot q+r_2$（$q\in\mathbf{Z},0\leqslant r_2<5$）。分别来计算 $f(i+j)$ 和 $f(i)+_5 f(j)$。

$$\begin{aligned}f(i+j)&=[(i+j)(\mathrm{mod}5)]\\&=[(r_1+r_2)(\mathrm{mod}5)]\\f(i)+_5 f(j)&=[i(\mathrm{mod}5)]+_5[j(\mathrm{mod}5)]\\&=[r_1]+_5[r_2]\\&=[(r_1+r_2)(\mathrm{mod}5)]\end{aligned}$$

因为 $f(i+j)=f(i)+_5 f(j)$，所以 f 是同态映射。

一般情况下，代数系统之间的同态映射并不是唯一的，并且在下一小节我们会知道上面这个例子就是所谓的自然同态。

定义 6.30 设$<X,*>$和$<Y,\triangle>$是两个代数系统，$f:X\to Y$ 是 X 到 Y 的同态映射。那么

1．若 f 是满射，则称 f 是**满同态**。

2．若 f 是双射，则称 f 是**同构映射**，并称代数系统$<X,*>$与$<Y,\triangle>$是**同构的**。记为 $X\cong Y$。

【例 6.25】 验证正实数的乘法群$<\mathbf{R}^+,\times>$和实数的加法群$<\mathbf{R},+>$是同构的。

解 考虑到两正实数的积的对数等于它们各自对数的和。令 $f(r)=\ln r$（$r\in\mathbf{R}^+$）。于是，

任取 $r_1 \in \mathbf{R}^+, r_2 \in \mathbf{R}^+$得

$$\ln(r_1 \times r_2) = \ln r_1 + \ln r_2$$

并且，因为对数函数是双射，所以$<\mathbf{R}^+, \times>$与$<\mathbf{R}, +>$是同构的。

在这里我们看到了全体实数和它的“一半”同构！

【例 6.26】 每一个 n 阶群都和一个 n 元置换群同构。

证明 设$<G, *>$是一个 n 阶群。我们可以构造一个 n 元置换群$<P, \circ>$，并证实在它们之间存在一个同构映射。对于每一个$a \in G$，定义一个 n 元置换 p_a，使得 G 中每一元素$c \in G$在置换 p_a 下的像，位于群 G 的复合表中元素 a 所在一行和 c 所在的列上。即，对任意$c \in G$，使得

$$p_a(c) = a * c$$

由本章定理 6.9 可知，这样恰好定义了 n 个不同的置换。所有这 n 个置换的集合就记为以上的 P。运算“$\circ$”就是普通置换（函数）的左复合运算。

首先，来证明$\langle P, \circ \rangle$的确是一个群。

设 $e \in G$ 是幺元。那么 $p_e \in P$ 就是 $<P, \circ>$ 的幺元。因为对任意 $a \in G$，$p_e \circ p_a = p_a \circ p_e = p_a$。实际上，按以上置换的定义，对任意 $x \in G$，有

$$p_e \circ p_a(x) = p_e(p_a(x)) = p_e(a * x) = e * (a * x) = a * x = p_a(x)$$

$$p_a \circ p_e(x) = p_a(p_e(x)) = p_a(e * x) = a * (e * x) = a * x = p_a(x)$$

类似地可证，对任意 $a \in G$，有

$$p_{a^{-1}} \circ p_a = p_a \circ p_{a^{-1}} = p_e$$

即每一个 $p_a \in P$，都有逆元 $p_{a^{-1}}$。

显然，对任意 $a \in G, b \in G, p_a \circ p_b = p_{a*b} \in P$（$\because a * b \in G$），故复合运算“$\circ$”在 P 上封闭。同时因为复合运算是满足结合律的，所以，$<P, \circ>$是 n **元置换群**。

然后，定义映射 $f: G \to P$：对 $a \in G$，使 $f(a) = p_a$。由定理 6.9 可知，若 $a \in G, b \in G$，且 $a \neq b$，则 $p_a \neq p_b$。因此，f 是双射。

最后，我们可以将以上的 $p_{a*b} = p_a \circ p_b$ 写成

$$f(a * b) = f(a) \circ f(b)$$

这就证明了 G 与 P 是同构的。

作为一个实例，读者不妨用本章 6.3 节表 6.7 给出的克莱茵 4 阶群复合表，构造一个与之同构的四元置换群（参考本章习题 6.46）。

定义 6.31 $<G, *>$是一代数系统，若存在自身上的映射 $f: G \to G$ 是同态映射，则称 f 是 G 的**自同态映射**。若 f 是同构映射，则称 f 是 G 的**自同构映射**。

两个同态或同构的代数系统之间有着重要的相似性。

定理 6.25 设$<H, *>$和$<K, \circ>$是两个代数系统，$f: H \to K$ 是 H 到 K 的同态映射。若$<H, *>$是群，则同态像 $f(H)$ 与运算“$\circ$”构成一个群$<f(H), \circ>$。

证明 逐一验证$<f(H), \circ>$具有群的 4 条基本性质。

运算$\circ$在 $f(H)$ 上是封闭的。任取 $x, y \in f(H)$，因为 $f(H)$ 是群的同态像，所以，有 $x = f(a), y = f(b)$（其中 $a \in H, b \in H$）。按照同态的定义，于是

$$x \circ y = f(a) \circ f(b) = f(a * b)$$

由于 $a * b \in H$，所以 $f(a * b) \in f(H)$，也即 $x \circ y \in f(H)$。

运算$\circ$满足结合律。任取 $x, y, z \in f(H)$，有 $a, b, c \in H$，使 $x = f(a)$，$y = f(b), z = f(c)$。

于是

$$\begin{aligned}(x\circ y)\circ z&=(f(a)\circ f(b))\circ f(c)\\&=f(a*b)\circ f(c)\\&=f((a*b)*c)\\&=f(a*(b*c))\\&=f(a)\circ f(b*c)\\&=x\circ(y\circ z)\end{aligned}$$

元素 $f(e)\in f(H)$ 是 $f(H)$ 的幺元（e 是群 H 的幺元）。任取 $x\in f(H)$，有 $a\in H$，使 $x=f(a)$。于是

$$\begin{aligned}f(e)\circ x&=f(e)\circ f(a)\\&=f(e*a)\\&=f(a)\\&=x\end{aligned}$$

同理可证 $x\circ f(e)=x$。这就是说，一个群的幺元的像就是该群同态像的幺元。

最后，每一个 $x\in f(H)$ 都有逆元，逆元是 $f(a^{-1})$。设 $x=f(a)(a\in H)$，因为

$$\begin{aligned}x\circ f(a^{-1})&=f(a)\circ f(a^{-1})\\&=f(a*a^{-1})\\&=f(e)\end{aligned}$$

所以，同态像 $<f(H),\circ>$ 是一个群。

从以上证明我们可以看出，同态映射将幺元 e 映射到幺元 $f(e)$，而且在群 H 中的两个互逆元素 a,a^{-1} 的像，仍是互逆的，即 $(f(a))^{-1}=f(a^{-1})$。

定义 6.32 设 f 是群 $<H,*>$ 到 $<K,\circ>$ 的一个同态。$f(e)=e'$ 是同态像 $f(H)$ 的幺元。H 中一切经 f 映射到 $e'\in K$ 的元素组成一个子集，该子集称为同态映射 f 的同态核。记为 $\mathrm{Ker}(f)$。即

$$\mathrm{Ker}(f)=\{x|x\in H,f(x)=f(e)=e'\}$$

定理 6.26 f 是由群 $<H,*>$ 到 $<K,\circ>$ 的同态。同态核 $\mathrm{Ker}(f)$ 是 H 的子群。

证明 任取 $a,b\in\mathrm{Ker}(f)$。按本章 6.3 节定理 6.13，只要证得 $a*b^{-1}\in\mathrm{Ker}(f)$，就证实了 $\mathrm{Ker}(f)$ 是 H 的子群。事实上，设 $e'=f(e)$ 是同态像的幺元。于是

$$\begin{aligned}f(a*b^{-1})&=f(a)\circ f(b^{-1})\\&=e'\circ(f(b))^{-1}\\&=e'\circ(e')^{-1}\\&=e'\end{aligned}$$

所以 $a*b^{-1}\in\mathrm{Ker}(f)$。

顺便指出，可以进一步证实 $\mathrm{Ker}(f)$ 还是 H 的一个正规子群。

关于同态核，我们可以看本节例 6.24。{…,-10，-5，0，5，10，…}就是例中映射 f 的同态核。

6.8.2 同余关系和同态

现在，我们换一个角度来考查同态。

定义 6.33 设 $<X,*>$ 是一个代数系统，R 是 X 上的一个等价关系。如果对任意

$x,y,u,v\in X$，且$<x,y>\in R$，$<u,v>\in R$，就有$<x*u,y*v>\in R$（就是说，在一个二元运算表达式$x*u$中，分别用与x同在一个等价类的元素y代替x，与u同在一个等价类的元素v代替u之后，运算结果$y*v$与$x*u$仍在一个等价类中。或者说从确定的两个等价类中各任取一个元素，它们的运算结果总是在同一个等价类中），则称等价关系R是X上**关于运算“*”的同余关系**。并且，由R诱导的等价类叫做**同余类**。

【例 6.27】 整数的加法群$<Z,+>$上的模 5 同余关系是同余关系[*]。

证明 沿用本节例 6.24 中的一些记号。设$a,b\in[i]$，$c,d\in[j]$，于是

$$a=5\cdot p_1+i \quad b=5\cdot p_2+i \quad c=5\cdot q_1+j \quad d=5\cdot q_2+j$$

所以

$$\begin{aligned}a+c&=(5\cdot p_1+i)+(5\cdot q_1+j)\\&=5(p_1+q_1)+(i+j)\\b+d&=(5\cdot p_2+i)+(5\cdot q_2+j)\\&=5(p_2+q_2)+(i+j)\end{aligned}$$

由以上结果可知$a+c$和$b+d$都在同余类$[(i+j)(\mathrm{mod}5)]$之中。

回到前面的例 6.24 中可见，$<\mathbf{Z},+>$上的同余关系，对应着一个从$\mathbf{Z}$到$\mathbf{Z}_5$的同态映射。

以下我们将证明任何一个同态都自然地和一个同余关系相对应。设$<X,*>$是一代数系统，E是X上的同余关系。可以定义一个商代数$<X/E,\triangle>$，其中二元运算$\triangle$是这样定义的：对任意$[x],[y]\in X/E$

$$[x]\triangle[y]=[x*y] \tag{6.24}$$

前面已经说过，在同余关系下，参与二元运算的元素在其各自的同余类中是任意可置换的，其结果均在同一个同余类中。所以运算$\triangle$的定义与同余类$[x]$和$[y]$以什么元素为代表元素无关。即，式（6.24）确实定义了一个二元运算（函数）。

再次，定义一个由$<X,*>$到$<X/E,\triangle>$的映射f_E，对任意$x\in X$，使得

$$f_E(x)=[x] \tag{6.25}$$

这样，式（6.24）就可以表示为

$$f_E(x)\triangle f_E(y)=f_E(x*y) \tag{6.26}$$

该式证实了f_E正是$<X,*>$到$<X/E,\triangle>$的一个同态，特别地称此同态为**自然同态**。

将以上结果写成定理形式如下：

定理 6.27 设E是代数系统$<X,*>$上的同余关系，存在一个由$<X,*>$到$<X/E,\triangle>$的同态。

进一步，我们来给出定理 6.27 的逆问题。

设f是由$<X,*>$到$<Y,\oplus>$的同态。定义X上的二元关系E_f如下

$$E_f=\{<x_1,x_2>\,|\,x_1,x_2\in X,f(x_1)=f(x_2)\} \tag{6.27}$$

显然，这样定义的二元关系是一个等价关系。我们来证明E_f是同余关系。任取x_1，x_2，$u_1,u_2\in X$，且$<x_1,x_2>\in E_f$，$<u_1,u_2>\in E_f$。由于f是同态，同时考虑E_f的定义，于是

$$f(x_1*u_1)=f(x_1)\oplus f(u_1)$$

[*] 在这里，前一个“同余关系”说的是关于整数除法狭义的同余关系；而后一个说的是一个代数系统上定义的一个等价关系诱导的商集的同余关系，商集有集合被“除分”的意思（参阅第 3 章 3.3.2 小节）。

$$= f(x_2) \oplus f(u_2)$$
$$= f(x_2 * u_2)$$

即 $< x_1 * u_1, x_2 * u_2 > \in E_f$。故 E_f 是同余关系。

实际上，我们已证明了以下定理：

定理 6.28 设 f 是代数系统 $< X, * >$ 到 $< Y, \oplus >$ 的同态。按公式（6.27）定义的二元关系是一个同余关系。

既然由 $< X, * >$ 到某个代数系统 $< Y, \oplus >$ 的满同态 f（为表述方便，这里设 f 为满同态）可以定义一个同余关系 E_f（被式（6.27）定义）。代数系统 $< X, * >$ 的每个同余关系 E 又都对应一个自然同态 f_E（满的）。如果我们将上述 X 上的同余关系 E 与用 X 到 Y 的满同态 f 定义的同余关系 E_f 用等式联系起来：即令 $E = E_f$。实际上，就是用由满同态 f 定义的同余关系 E_f，按照式（6.25）定义自然同态 $f_{E_f} : X \to X / E_f$。于是自然想到可以定义一个 $X / E_f \to Y$ 的双射 h（参考图 6.4）：对任意 $x \in X$，使得

$$h([x]) = f(x) \tag{6.28}$$

可以证明 h 是 $< X / E_f, \triangle >$（其中运算“$\triangle$”如公式（6.24）定义）到 $< Y, \oplus >$ 的同构映射。因为对任意 $x_1, x_2 \in X$，我们有

$h([x_1] \triangle [x_2]) = h(f_E(x_1) \triangle f_E(x_2))$ （根据式（6.25））
$= h(f_E(x_1 * x_2))$ （根据式（6.26））
$= h([x_1 * x_2])$ （根据式（6.25））
$= f(x_1 * x_2)$ （根据式（6.28））
$= f(x_1) \oplus f(x_2)$ （f 是 $X \to Y$ 的同态）
$= h([x_1]) \oplus h([x_2])$ （根据式（6.28））

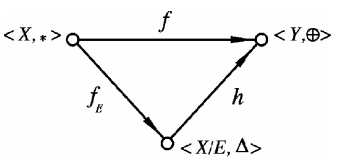


图 6.4

注意：以上推导中的 f_E 实际上就是 f_{E_f}。

6.9 环和域

本节来讨论定义了两个二元运算的代数系统。

定义 6.34 设 R 是非空集，“$\oplus$”和“$*$”是两个定义在 R 上的封闭的二元运算。如果它们满足以下规律：

（1）$< R, \oplus >$ 构成交换群。

（2）$< R, * >$ 构成半群。

（3）乘法 $*$ 对加法 $\oplus$ 满足分配律。

则称代数系统 $< R, \oplus, * >$ 是**环**。

习惯上，我们称这里第一个二元运算为“加法”，第二个为“乘法”。

例如，对于实数 **R** 的普通加法和乘法，$<\mathbf{R}, +, \times >$ 是一个环。整数集 **Z** 构成 $<\mathbf{Z}, +, \times >$ 也是环，复数集 **C** 构成环 $<\mathbf{C}, +, \times >$。

【例 6.28】 元素全是实数的 n 阶实数矩阵的集 A_n，连同矩阵的加法和乘法构成 n 阶矩阵环 $< A_n, +, \cdot >$。

【例 6.29】 关于字母 x 的整数系数的多项式的集 $F[x]$ 在多项式加法和乘法下构成多项式环 $< F[x], +, \cdot >$。

由于在一个环$<R,\oplus,*>$上，$<R,*>$是半群，$*$ 运算满足结合律，所以对$a\in R$，可定义幂a^m（m是正整数）。同时有

$$a^m * a^n = a^{(m+n)} \qquad (a^m)^n = a^{mn}$$

如果运算 $*$ 是可交换的，对$a,b\in R$，还有

$$(a*b)^m = a^m * b^m$$

具有可交换乘法“$*$”的环叫做**交换环**。

我们约定，环$<R,\oplus,*>$中，R关于加法$\oplus$的幺元记为θ。元素$x\in R$的加法逆元记为$-x$，即$x+(-x)=\theta$。也可以将$x+(-y)$简记成$x-y$。

我们还约定，乘法运算优先于加法运算。

定理 6.29 设$<R,+,\cdot>$是环。对于任意$x,y,z\in R$，有

1．$x\cdot\theta=\theta\cdot x=\theta$。

2．$x\cdot(-y)=(-x)\cdot y=-(x\cdot y)$。

3．$(-x)\cdot(-y)=x\cdot y$。

4．$x\cdot(y-z)=x\cdot y-x\cdot z$。

5．$(x-y)\cdot z=x\cdot z-y\cdot z$。

证明 以上所有结论在实数环中都是我们熟悉的。但对一般的环，它们并非显然的。现证明如下。

（1）因为

$$x\cdot\theta=x\cdot(\theta+\theta)=x\cdot\theta+x\cdot\theta$$

而群$<R,+>$有唯一的幂等元是幺元（见本章定理 6.10），所以，$x\cdot\theta=\theta$。同理可证$\theta\cdot x=\theta$。

（2）因为$x\cdot(-y)+x\cdot y=x\cdot((-y)+y)=x\cdot\theta=\theta$。可见$x\cdot(-y)$是$x\cdot y$的逆元，即$x\cdot(-y)=-(x\cdot y)$。

（3）类似（2）证明。

（4）$x\cdot(y-z)=x\cdot(y+(-z))=x\cdot y+x\cdot(-z)=x\cdot y+(-(x\cdot z))=x\cdot y-x\cdot z$。

（5）类似证明（4）。

由以上的（1）可知，一个环的加法幺元θ，就是乘法的零元。

定义 6.35 若环$<R,+,\cdot>$中含有关于乘法的幺元（记做 1），则环$<R,+,\cdot>$叫做**含幺环**。

类似于定理 6.1 可证含幺环的乘法幺元是唯一的。

若环R含有不止一个元素，则乘法幺元一定不等于加法幺元。因为若不然，$1=\theta$，则对$x\in R$，有

$$x=1\cdot x=\theta\cdot x=\theta$$

这就是说环R只含有一个元素θ，矛盾。

定义 6.36 $<R,+,\cdot>$是环。若$x,y\in R,x\neq\theta,y\neq\theta$，但$x\cdot y=\theta$，则称$x,y$是环$R$的**零因子**。

关于环的乘法也有可约律，但这与群的可约律有很重要的区别。由于乘法有零元θ，因此可约律可表达为$x\cdot z=y\cdot z$，当$z\neq\theta$，则$x=y$。环的乘法可约律必须满足以下条件。

定理 6.30 $<R,+,\cdot>$是无零因子的环，当且仅当对乘法满足可约律。

证明 必要性。

设$<R,+,\cdot>$是无零因子的环。来证对乘法可约律成立。设有$x\cdot z=y\cdot z$，且$z\neq\theta$。有$x\cdot z+(-(y\cdot z))=\theta$，也就是$x\cdot z-y\cdot z=(x-y)\cdot z=\theta$。因为无零因子，且$z\neq\theta$，所以$x-y=\theta$或$x+(-y)=\theta$。即$x$是$-y$的逆元，同时$y$的逆元是$-y$。由于逆元是唯一的，所以$x=y$。

充分性。

假设可约律对于乘法成立。要证 R 不含零因子。设 $x,y\in R, x\cdot y=\theta$，且 $x\neq\theta$。则 $x\cdot y=\theta=x\cdot\theta$，消去 x 后得 $y=\theta$，即 R 没有零因子。

定义 6.37 若环 $<R,+,\cdot>$ 有乘法幺元 1，无零因子，且乘法有交换律，则称 R 为**整环**。

前面提到的整数环$<\mathbf{Z},+,\times>$、实数环$<\mathbf{R},+,\times>$和复数环$<\mathbf{C},+,\times>$均为整环。

【例 6.30】 在例 6.28 中提到的 n 阶矩阵环 $<A_n,+,\cdot>$ 不是整环。

证明 令 $n=2$，举一反例

$$\begin{bmatrix}2 & 1\\ 2 & 1\end{bmatrix}\cdot\begin{bmatrix}-2 & 3\\ 4 & -6\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

而等式右边的矩阵恰是 A_2 环的零元。这就是说，环 $<A_2,+,\cdot>$ 含有零因子。

域是一种特殊的环。有时，在环 $<R,+,\cdot>$ 中，若排除乘法的零元 θ（即加法幺元），$<R-\{\theta\},\cdot>$ 可能成为一个群。在这样的处理下，乘法可具有很多其他性质。

定义 6.38 设 $<A,+,\cdot>$ 是一代数系统。如果

（1）$<A,+>$ 是交换群。

（2）$<A-\{\theta\},\cdot>$ 是交换群。

（3）运算乘法对加法有分配律。

则称 $<A,+,\cdot>$ 是**域**。

实数环和复数环都是域。特别要指出的是，整数环不是域，因为$<\mathbf{Z}-\{0\},\cdot>$不是群。

关于整环和域有一些关系。

定理 6.31 域一定是整环。

证明 由整环的定义可知，只要证明域不含零因子就行了。而根据定理 6.30 只要证明域满足乘法的可约律。

设 $<A,+,\cdot>$ 是域，若 $x,y,z\in A, x\neq\theta$, 且 $x\cdot y=x\cdot z$，则

$$\begin{aligned}y&=1\cdot y=(x^{-1}\cdot x)\cdot y\\&=x^{-1}\cdot(x\cdot y)\\&=x^{-1}\cdot(x\cdot z)\\&=(x^{-1}\cdot x)\cdot z\\&=z\end{aligned}$$

其中 x^{-1} 表示 x 关于乘法的逆元。

一般而言，定理 6.31 的逆定理不成立，但是，对于有限整环有以下定理。

定理 6.32 有限整环是域。

证明 设 $<A,+,\cdot>$ 是有限整环。由整环和域的定义可知，这里只要证明有限整环的每一非零元都有乘法逆元。

任取 $x\in A-\{\theta\}$，$y,z\in A-\{\theta\}$。若 $y\neq z$，那么 $x\cdot y\neq x\cdot z$（因为整环有关于乘法可约律）。又因整环是无零因子的，所以乘法在 $A-\{\theta\}$ 上封闭。根据本章 6.6 节关于两个集合之积的定义 6.26，有 $(A-\{\theta\})\{x\}=A-\{\theta\}$。

又设 1 是关于乘法的幺元。由以上等式和有限环的假设可以肯定，必有 $w\in A-\{\theta\}$，使 $w\cdot x=1$。故 w 就是 x 的关于乘法的逆元。

可以将同态的概念推广到环上来。

定义 6.39 设 $<X,+,\cdot>$ 和 $<Y,\oplus,*>$ 是各有两个二元运算的代数系统。$f:X\to Y$ 是映射。

若对任意 $x,y\in X$，有

$$f(x+y)=f(x)\oplus f(y)$$
$$f(x\cdot y)=f(x)*f(y)$$

则称 f 是 $<X,+,\cdot>$ 到 $<Y,\oplus,*>$ 的同态映射。像集 $f(X)\subseteq Y$ 是 $<X,+,\cdot>$ 的同态像。

定理 6.33 设 f 是环 $<R,+,\cdot>$ 到 $<L,\oplus,*>$ 上的满同态，则 $<L,\oplus,*>$ 也是环。

证明 由于 $<R,+,\cdot>$ 是环，所以 $<R,+>$ 是交换群，$<R,\cdot>$ 是半群。根据本章 6.8 节定理 6.25 的证明可知，在同态 f 下，同态像 $<L,\oplus,*>$ 中的 $<L,\oplus>$ 一定是交换群，$<L,*>$ 一定是半群。

剩下的只要证明在 $<L,\oplus,*>$ 中，运算 $*$ 对 $\oplus$ 满足分配律。任取 $u,v,w\in L$，有 $x,y,z\in R$。使 $u=f(x)$，$v=f(y)$，$w=f(z)$。于是

$$\begin{aligned}u*(v\oplus w)&=f(x)*(f(y)\oplus f(z))\\&=f(x)*f(y+z)\\&=f(x\cdot(y+z))\\&=f(x\cdot y+x\cdot z)\\&=f(x\cdot y)\oplus f(x\cdot z)\\&=f(x)*f(y)\oplus f(x)*f(z)\\&=u*v\oplus u*w\end{aligned}$$

习　题

6.1　设 C 是上衣和裤子的集合。设 $S=\{F,T\}$。现在请定义一个 C 到 S 的二元运算，并使这个运算具有某种实际意义。

6.2　设 $N=\{1,2,3,\cdots\}$，定义四个运算：

（a）$a*b=\gcd(a,b)$，（b）$a\square b=|a-b|$

（c）$a\triangle b=a^b$，　（d）$a\oplus b=ab+a$

其中 $\gcd(a,b)$ 是 a 与 b 的最大公因数。试问这几个运算是否为封闭的？可结合的？可交换的？哪一种运算在 N 上有幺元？有的话幺元是什么？

6.3　说明以下判断的正误，并说出理由。

（a）加法是自然数上的运算。

（b）减法是自然数到整数上的运算。

（c）除法是有理数上的运算。

（d）整数集在减法下是一个代数系统。

（e）设 E 是偶数集合，令一元运算 $*x=5x$，则 $<E,*>$ 是一代数系统。

（f）有理数上的取算术根的运算构成一个代数系统。

6.4　举出三个代数系统的例子。

6.5　试求出半群 $<\rho(X),\bigcap>$ 和 $<\rho(X),\bigcup>$ 的所有零元，其中 X 表示任意集合，$\rho(X)$ 是其幂集，它们是独异点吗？如果是的话，试求出幺元。

6.6　试证自然数集合 $\mathbf{N}=\{0,1,2,3,\cdots\}$ 关于运算 $x*y=\max\{x,y\}$ 是一半群。它是独异点吗？

6.7　设 z 是可交换半群 S 的左零元，试证对任一 $x\in S$，$z*x$ 和 $x*z$ 也是左零元。

6.8　设 $\mathbf{Z}$ 是整数集合，而“$\circ$”是乘法运算，因而$<\mathbf{Z},\circ,1>$是独异点。证明$<\mathbf{E},\circ>$是子

半群但不是子独异点，其中 **E** 表示偶数集合。

6.9 设 $Z_n=\{0,1,2,\cdots,n-1\}$，“$*$”是 Z_n 上的二元运算，令

$$a*b=(a\cdot b)(\mathrm{mod}\,n)$$

（a）对 $n=4$，列出运算 $*$ 的复合表。

（b）对任何 n，证明 $<Z_n,*>$ 是半群。

6.10 设 $<X,*>$ 是半群，a 是 X 的一个元素，X 上的二元运算△，使任意 $x,y\in X$ 有

$$x\triangle y=x*a*y$$

证明△是 X 上的可结合运算。

6.11 设 $<\{a,b\},*>$ 是一个半群，有 $a*a=b$。证明：

（a）$a*b=b*a$，（b）$b*b=b$

6.12 设 $<X,*>$ 是可交换半群，证明：如果 $a*a=a,b*b=b$，则 $(a*b)*(a*b)=a*b$

6.13 设 $<X,*>$ 是一个有限半群，证明该半群必有幂等元 a，即 $a*a=a$。

6.14 设 $<X,*>$ 是一个半群，存在 $a\in X$，使得对于每一个 $x\in X$，都可以找出 $u,v\in X$，满足等式

$$a*u=v*a=x$$

证明：X 有一个幺元（**提示**：对于 a 可找到 a' 和 a''，使 $a*a'=a''*a=a$。于是可证明 a' 是右幺元而 a'' 是左幺元）。

6.15 试证：独异点的所有逆元的元素的集合，连同独异点上的运算构成一个群。

6.16 若 $<G,*>$ 和 $<H,*>$ 都是群 $<X,*>$ 的子群，那么 $<G\cup H,*>$ 是否一定也是 $<X,*>$ 的子群？说明理由。

6.17 设 $<G,*>$ 是群，对任一个 $a\in G$，令

$$H=\{y|y*a=a*y,y\in G\}$$

证明 $<H,*>$ 是 G 的子群。

6.18 试证：x 的所有整系数多项式 $F[x]$ 在加法运算下构成一个群。

6.19 设 $<G,*>$ 和 $<H,\circ>$ 是两个群，定义它们的笛卡尔积为代数系统 $<G\times H,\triangle>$，在这里△是 $G\times H$ 上的二元运算，它使任何 $<x,u>,<y,v>\in G\times H$ 有

$$<x,u>\triangle<y,v>=<x*y,u\circ v>$$

证明：$<G\times H,\triangle>$ 是一个群。

6.20 设 $<G,*>$ 是群，证明：

（a）$(a_1*a_2*\cdots*a_r)^{-1}=a_r^{-1}*\cdots*a_2^{-1}*a_1^{-1}$

（b）$(a^i*b^j)^{-1}=b^{-j}*a^{-i}$

其中 i 和 j 是任意整数。

6.21 设 H_1 和 H_2 都是群 G 的子群，且彼此互不包含，证明存在一个元素 $a\in G$，它不属于 H_1 和 H_2 中任一个。

6.22 设 $<G,*>$ 是一个群，$|G|$ 是偶数，证明有一个 $a\in G$，它的逆元是其自身，即 $a=a^{-1}$，且 a 不是幺元（参考 6.3.1 小节克莱茵群的复合表，表 6.7）。

6.23 给出克莱茵四阶群（见表 6.7）的所有循环子群。

6.24 设 $<H,*>$ 和 $<G,*>$ 都是群 $<S,*>$ 的子群，令

$$HG=\{h*g|h\in H,g\in G\}；$$

证明：$<HG,*>$ 是 S 的子群的充分必要条件是 $HG=GH$。

6.25　证明：任何循环群的子群一定也是循环群。

6.26　求置换 $\tau=(1\ 2\ 3)\circ(2\ 4\ 3)\circ(1\ 3)\circ(1\ 4)$下，元素 1,2,3,4 的像。

6.27　求置换的幂

$$\begin{bmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 5 & 3 & 1\end{bmatrix}^6$$

6.28　设 $\sigma=(1\ 3\ 2)$，$\tau=(1\ 3)(2\ 4)$。求 $\sigma\circ\tau\circ\sigma^{-1}$ 和 $\sigma^{-1}\circ\tau\circ\sigma$。

6.29　设置换 $\sigma=\sigma_1\circ\sigma_2\circ\cdots\sigma_r$，其中 $\sigma_i(1\leqslant i\leqslant r)$都是轮换。证明：

（a）$\sigma^{-1}=\sigma_r^{-1}\circ\sigma_{r-1}^{-1}\circ\cdots\circ\sigma_2^{-1}\sigma_1^{-1}$

（b）若 $\sigma_i(1\leqslant i\leqslant r)$ 全是不相杂的，证明：$\sigma^{-1}=\sigma_1^{-1}\circ\sigma_2^{-1}\circ\cdots\circ\sigma_r^{-1}$

6.30　设 $A=\{a,b,c,d,e\}$ 上有四个置换如下

$$\alpha=\begin{pmatrix}a & b & c & d & e\\ b & c & a & d & e\end{pmatrix},\qquad \beta=\begin{pmatrix}a & b & c & d & e\\ a & b & c & e & d\end{pmatrix},$$

$$\gamma=\begin{pmatrix}a & b & c & d & e\\ e & d & c & b & a\end{pmatrix},\qquad \delta=\begin{pmatrix}a & b & c & d & e\\ c & b & a & e & d\end{pmatrix}。$$

试在对称群 A_5 中求 $\alpha\circ\beta,\beta\circ\alpha,\alpha\circ\alpha,\gamma\circ\beta,\beta^{-1},\alpha\circ\beta\circ\gamma$, 并求方程 $\alpha\circ x=\delta$ 的解。

6.31　在一张卡片上打印十进制的 5 位数，对于小于 10000 的数在高位上添上 0 凑足 5 位。若一个数上下颠倒地看仍是一个数，就只打印在一张卡片上（如 69016 倒过来看 91069），问需要多少张卡片才能打印所有 5 位数？

6.32　设 G 是所有实系数非退化一次函数 $f(x)=ax+b$（$a,b\in R$，$a\neq 0$）的集合。运算$\circ$是函数的左复合运算。证明：

（a）$<G,\circ>$是一个群。

（b）若 S 是所有 $f(x)=x+b\ (b\in R)$ 的集合，H 是所有 $g(x)=ax$（$a\in R,a\neq 0$）的集合，则$<S,\circ>$和$<H,\circ>$构成$<G,\circ>$的子群。

（c）写出 S 和 H 在 G 中的所有左陪集。

6.33　设$<G,*>$是一个群，定义一个二元关系：

$$R=\{<x,y>\,|(\exists u)(u\in G\ \wedge\ y=u*x*u^{-1}\}$$

证明 R 是 G 上的等价关系。

6.34　设 $S=\{1,2,3,4\}$，σ 是 S 上的置换

$$\sigma=(1\ 4\ 2\ 3)$$

求由 σ 生成的循环群，并写出该循环群的所有左陪集和右陪集，最后判断此循环群是否为正规子群。

6.35　继续证明题 6.17 中的子群$<H,*>$也是正规子群。

6.36　设$<H,*>$是群$<G,*>$的子群，$<N,*>$是$<G,*>$的正规子群。证明$<HN,*>$是$<G,*>$的子群（对照习题 6.24）。

6.37　设 $S=\{1,2,3,4\}$，$<S_n,\circ>$是 S 上的对称群。令 $H=\{I_s,(1\ \ 2)\circ(3\ \ 4),(1\ \ 3)\circ(2\ \ 4),(1\ 4)\circ(2\ 3)\}$，证明$<H,\circ>$是$<S_n,\circ>$的正规子群。

6.38　证明循环群的任何子群一定是正规子群。

6.39　设 p 是一个质数，m 是正整数，证明一个 p^m 阶群一定有 p 阶的子群。

6.40　设 f 是群$<G,*>$到$<H,\circ>$的满同态。证明 f 的同态核$<\mathrm{Ker}(f),*>$是 G 的正规子群。

6.41　设 H 是群$<G,*>$的一个正规子群。证明 G 上的关系（同属一个左陪集的关系）

$$R=\{<x,y>\,|\,x\in G\ \wedge\ y\in G\ \wedge\ (\exists h)(h\in H\ \wedge\ x*h=y)\}$$

是同余关系。

6.42　设 H 是交换群 $<G,*>$ 的正规子群。S 是 H 在群 G 的所有左陪集的集合。证明由 H 诱导的自然同态像 $<S,\triangle>$ 也是交换群。其中，运算“$\triangle$”定义由等式 $aH\triangle bH=(a*b)H$ 给出。又若 G 不是交换群，可是对任意元素 $x,y\in G$，若 $x*y*x^{-1}*y^{-1}\in H$，则由正规子群 H 诱导的自然同态像 $<S,\triangle>$ 仍然是交换群（参考题 6.41 的结果）。

6.43　设 f 是从 $<X,*>$ 到 $<Y,\triangle>$ 的同态映射，h 是从 $<Y,\triangle>$ 到 $<Z,\circ>$ 的同态映射，证明 $h\circ f$ 是从 $<X,*>$ 到 $<Z,\circ>$ 的同态映射。

6.44　设 f 是从 $<X,*>$ 到 $<Y,\circ>$ 的同构映射，证明 f^{-1} 是从 $<Y,\circ>$ 到 $<X,*>$ 的同构映射。

6.45　设 $<G,*>$ 是一个群，$a\in G$。若 f 是一个 G 到自身的映射，使对每一个 $x\in G$ 有

$$f(x)=a*x*a^{-1}$$

证明：f 是 G 的自同构（自同构的定义是 G 在同构映射下的像 $f(G)$ 与 G 同构）。

6.46　证明克莱茵四阶群与置换群 $<G,\circ>$ 是同构的。$G=\{p_1,p_2,p_3,p_4\}$，其中运算“$\circ$”是置换的复合，而每一置换如下给出

$$p_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\qquad p_2=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},$$

$$p_3=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\qquad p_4=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}。$$

参阅本章例题 6.26。

6.47　设 f,g 都是从群 $<G,*>$ 到群 $<H,\circ>$ 的同态映射，证明 $<C,*>$ 是 $<G,*>$ 的子群。其中

$$C=\{x\,|\,x\in G\wedge f(x)=g(x)\}$$

6.48　设 f 是从群 $<G,*>$ 到 $<S,\circ>$ 的同态映射，则 f 是入射的充分必要条件是 $\mathrm{Ker}(f)=\{e\}$，e 是群 G 的幺元（**提示**：参考题 6.40 的结果）。

6.49　证明代数系统 $<X,*>$ 上的两个同余关系 R_1 和 R_2 的交 $R_1\cap R_2$ 关系也是同余关系。

6.50　设 $<X,\oplus,*>$ 是一个代数系统，对于 $x,y\in X$，式 $x\oplus y=x$ 总成立，而“$*$”是任意二元运算，证明“$*$”对“$\oplus$”运算是可分配的。

6.51　设 $<R,+,\circ>$ 是一个环，所有元素 $x\in R$ 对乘法都是幂等元，即 $x\circ x=x$。证明：

（a）对于所有 $x\in R$，有 $x+x=\theta$，其中 θ 是加法的幺元。

（b）乘运算是可交换的。

6.52　试构造一个由两个元素组成的集 $R=\{e,a\}$ 上的环 $<R,+,\circ>$。能构造 R 为整环吗？给出“+”和“$\circ$”两个运算的复合表（**提示**：环必须满足乘法对加法的分配律）。

6.53　设 $<A,+,\circ>$ 是定义了普通加法和乘法的代数系统，A 分别表示以下各集合

（a）$A=\{x\,|\,x\geqslant 0,x\in\mathbf{Z}\}$　　（$\mathbf{Z}$ 为整数集合）

（b）$A=\{x\,|\,a+b\sqrt{3},a,b\in\mathbf{Q}\}$（$\mathbf{Q}$ 为有理数集合）

（c）$A=\{x\,|\,a+b\sqrt[3]{5},a,b\in\mathbf{Q}\}$（$\mathbf{Q}$ 为有理数集合）

问 $<A,+,\circ>$ 在以上各种情况下是否是整环？是否是域？说明理由。

第 7 章　格与布尔代数

1854 年，乔治·布尔（Geoge　Boole）首先提出了一种后来被称为**布尔代数**的理论。布尔代数是一种特殊的代数系统，与逻辑、集合的运算有密切的关系。

有一种叫做**格代数**的系统，格代数与一种特殊的偏序集有着紧密的关联，因为这种偏序集与格代数互为对应物。而布尔代数是格代数的一种特殊形式。

因此，以下的讨论就从某种特殊的偏序集开始，然后转入格代数，最后专门讨论布尔代数的一些性质。

布尔代数在计算机的理论和设计中起着很重要的作用，在数字电路的简化和其他科学和工程领域内也有广泛的应用。

7.1　偏序集、格和格代数

7.1.1　偏序和格

在第 3 章，我们讨论过集合 A 上的偏序关系“$\leqslant$”。用序偶 $<A,\leqslant>$ 标识一个偏序集。并且知道，在 A 的一个子集 $B\subseteq A$ 上，不必有最大下界（下确界 inf）和最小上界（上确界 sup）。如图 7.1 是一个偏序的哈斯图。子集 $\{a,b\}$ 有 3 个下界，c 是下确界，但没有上确界（甚至不存在上界）。而子集 $\{d,e\}$ 恰好相反，没有下确界，却有上确界 c。

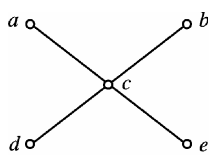


图 7.1　偏序集

在这里，我们关注的是这样一类偏序，即偏序集中的任何两个元素组成的子集都有一个下确界和一个上确界，这样的偏序叫做**格**。今后，我们将一个偏序集的由两个元素组成的子集 $\{x,y\}$ 的上（下）确界就称为“元素 x 和 y 的上（下）确界”。

定义 7.1　$<A,\leqslant>$ 是**偏序格**，如果其任意两个元素 $x,y\in A$，在 A 上都有一个上确界和一个下确界。偏序格简称为**格**。

$x,y\in A$，用 $\inf\{x,y\}$ 记 x 与 y 的下确界，用 $\sup\{x,y\}$ 记 x 和 y 的上确界。

以下是两个格的例子。

【例 7.1】　设 $\rho(X)$ 表示集合 X 的幂集。那么 $<\rho(X),\subseteq>$ 是格。

证明　因为对任意 A_i，$A_j\in\rho(X)$，$\inf\{A_i,A_j\}=A_i\cap A_j$。实际上 $A_i\cap A_j\subseteq A_i$，$A_i\cap A_j\subseteq A_j$（见第 3 章 3.1.2 小节式(3.10)），且若 A_k 也是 A_i，A_j 的下界，即 $A_k\subseteq A_i$，$A_k\subseteq A_j$。设若 $x\in A_k$，则 $x\in A_i$ 和 $x\in A_j$，就是 $x\subseteq A_i\cap A_j$，即 $A_k\subseteq A_i\cap A_j$。由此说明 $A_i\cap A_j$ 是 A_i 和 A_j 的最大下界。类似有 $\sup\{A_i,A_j\}=A_i\cup A_j$。所以 $<\rho(X),\subseteq>$ 是格。

图 7.2 是当 $X=\{a,b,c\}$ 时，格 $<\rho(X),\subseteq>$ 的哈斯图。

【例 7.2】　若将命题逻辑中所有主析（合）取范式相同的等价式均以主析（合）取范式表示，那么全体合式公式的集 F 和其上的蕴含关系“$\Rightarrow$”构成偏序格 $<F,\Rightarrow>$。

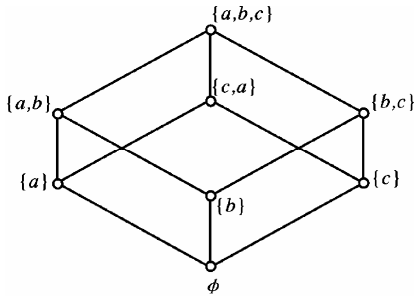


图 7.2　格的例子

证明　因为对任意两个主范式 f_1，$f_2 \in F$，一方面 $f_1 \wedge f_2 \Rightarrow f_1$，$f_1 \wedge f_2 \Rightarrow f_2$。另一方面，若有 $f' \in F$，且 $f' \Rightarrow f_1$ 和 $f' \Rightarrow f_2$，则 $f_1 \Rightarrow f_1 \wedge f_2$。所以 $\inf\{f_1, f_2\} = f_1 \wedge f_2$，类似地，$\sup\{f_1, f_2\} = f_1 \vee f_2$。

图 7.3 给出了一些偏序的哈斯图，通过直接验证可知它们都是格。而图 7.4 中的每一个偏序关系都不是格。

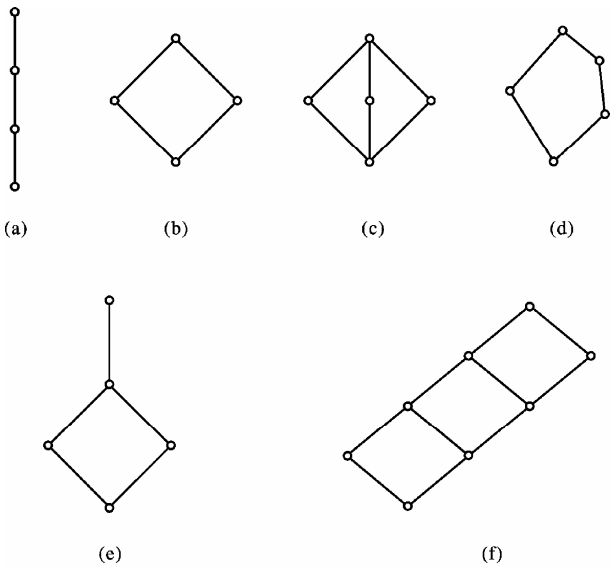


图 7.3　一些偏序格

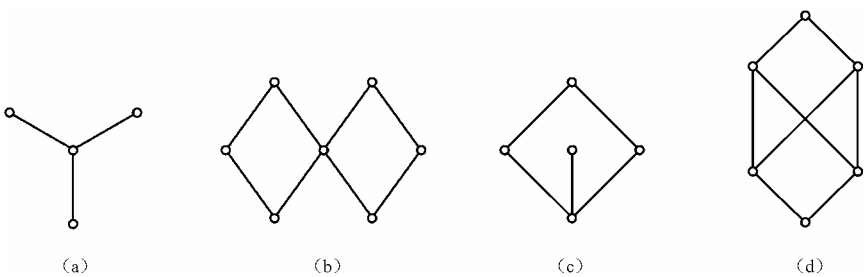


图 7.4　不是格的偏序集

顺便提一下，要直观地通过哈斯图验证一个偏序是否是格，可以这样做：任意找两个结点，从它们中的每一个开始，尽可能地沿着哈斯图中的边上行（下行），直至汇合在唯一的一

点上，或者这样做不能汇合于哈斯图的一点上，或者可以汇合在多个点上，且其中有两个汇合点是不可比的。第一种情况下，交汇点就是原先两结点的上（下）确界，后一种情形则没有上（下）确界。以此可判断一偏序是或不是格。

7.1.2 对偶原理

设$<A,\leq>$是偏序集。由第 3 章习题 3.41(b)可知，关系“$\leqslant$”的逆“$\geqslant$”也是偏序关系。容易明白，这时$<A,\geqslant>$的哈斯图可通过颠倒$<A,\leqslant>$的哈斯图得到。而且元素$x,y\in A$在$<A,\leqslant>$上的上确界恰恰是它们在$<A,\geqslant>$中的下确界，在$<A,\leqslant>$中的下确界就是在$<A,\geqslant>$中的上确界。所以，当$<A,\leqslant>$是格时，$<A,\geqslant>$也是格。反之亦然。可以想像，在格$<A,\leqslant>$中的每一个描述或命题，必然以一种对偶的方式存在于格$<A,\geqslant>$之中。这就是所谓的对偶原理。可以用一个有趣的例子来诠释对偶原理。在欧洲大陆上，交通规则可简要地描述为：“车辆必须沿道路右侧行驶。驾驶者的座位在车辆的左侧。当遭遇红灯时车辆仅可以继续右转弯行驶，遭遇绿灯时可以直行或不影响对面直行车辆行驶的情况下左转弯行驶。”若将以上规则中出现的“左”改为“右”，而“右”改为“左”，那么就立即成为在英国驾驶员应遵守的交通规则了。

定理 7.1（对偶原理）每一个关于格的上、下确界以及偏序关系“$\leqslant$”，“$\geqslant$”的命题是真命题，当且仅当将命题中的上确界换成下确界，下确界换成上确界，将关系“$\leqslant$”换成“$\geqslant$”，将“$\geqslant$”换成“$\leqslant$”后是一个真命题。

我们把关系“$\leqslant$”和“$\geqslant$”，两个元素的上确界和下确界，偏序格$<A,\leqslant>$和$<A,\geqslant>$统统称为是相互对偶的。

7.1.3 格的初等性质

在格$<A,\leqslant>$上，因为任何两个元素$x,y\in A$的上、下确界都各是唯一的，所以可以将上、下确界看成是两个元素x和y的二元运算的结果。

我们约定，用“$\oplus$”号表示求两元素上确界的运算，即$x\oplus y=\sup\{x,y\}$。用“$\cdot$”号表示求两元素下确界的运算，即$x\cdot y=\inf\{x,y\}$，并直呼“$\oplus$”为“加法”，“$\cdot$”为“乘法”。在不致引起混淆的情况下，还可将$x\cdot y$记为xy，并且，规定“乘法”运算优先于“加法”。

定理 7.2 设$x,y,z\in A$是格$<A,\leqslant>$的任意元素。以下等式恒成立。

（1）$xx=x$	（1'）$x\oplus x=x$	（7.1）
（2）$xy=yx$	（2'）$x\oplus y=y\oplus x$	（7.2）
（3）$(xy)z=x(yz)$	（3'）$(x\oplus y)\oplus z=x\oplus(y\oplus z)$	（7.3）
（4）$x(x\oplus y)=x$	（4'）$x\oplus xy=x$	（7.4）

以上 4 个等式依次描述的是格的**幂等律**、**交换律**、**结合律**和**吸收律**。上述左边一栏的 4 个公式可以从$\oplus$与$\cdot$的定义直接证明。这之后，从对偶原理可知，以上右边一栏的 4 个分别与之对偶的公式自然就成立了。

证明 我们以公式（7.4）的（4）为例给出一个证明。

设$x,y\in A$，根据“$\oplus$”的定义有$x\leqslant x\oplus y$。又因<A，$\leqslant$>是偏序，所以$x\leqslant x$，即x是x和$x\oplus y$的一个下界，自然$x\leqslant x(x\oplus y)$。另外，$x(x\oplus y)$是x和$x\oplus y$的下确界——最大下界，按下确界的定义可知$x(x\oplus y)\leqslant x$（两元素的任何下界都“小于等于”每一个元素），结合刚才证得的$x\leqslant x(x\oplus y)$，并且因为偏序关系“$\leqslant$”是反自反的，所以$x=x(x\oplus y)$。

定理 7.3 设 $x,y\in A$ 是格 $<A,\leqslant>$ 的任意元素。则

$$(x\leqslant y)\Leftrightarrow(xy=x)\Leftrightarrow(x\oplus y=y) \tag{7.5}$$

证明 只要证 $(x\leqslant y)\Leftrightarrow(xy=x)$，通过对偶原理可得 $(x\geqslant y)\Leftrightarrow(x\oplus y)=x$。因 x,y 是任意元素，所以上式将 x,y 互换后，也可写成 $(x\leqslant y)\Leftrightarrow(x\oplus y=y)$。最后因为等价关系是对称的和传递的，终于得出式（7.5）。

设 $x\leqslant y$，来证 $xy=x$。由 $x\leqslant y$，还因 $x\leqslant x$，所以 $x\leqslant xy$（x 是 x,y 的下界，而下界“小于等于”下确界）。可是根据下确界的定义，应该有 $xy\leqslant x$，这样就得 $xy=x$。

又设 $xy=x$，来证 $x\leqslant y$。事实上，这里的假设可直接推知 $x\leqslant y$，因为 $xy=x$ 表示 x 是 x 和 y 的下确界。

定理 7.2 和定理 7.3 是建立格与布尔代数的基础，我们应当透彻地理解它们。

定理 7.4 设$<A,\leqslant>$是格。$x,y,z\in A$ 是 A 的任意元素。则

$$(y\leqslant z)\Rightarrow(xy\leqslant xz)\wedge(x\oplus y)\leqslant(x\oplus z) \tag{7.6}$$

等式（7.6）又被称为格的“保序性”。

证明 设 $y\leqslant z$。由定理 7.3 有 $yz=y$。而应用结合律、交换律和幂等律，有

$$\begin{aligned}(xy)\cdot(xz)&=(xx)\cdot(yz)\\&=xy\end{aligned}$$

所以由定理 7.3 可知，$xy\leqslant xz$。

同理可证 $(y\leqslant z)\Rightarrow(x\oplus y)\leqslant(x\oplus z)$。当然也可应用对偶原理从以上已证的蕴含式 $(y\leqslant z)\Rightarrow(xy\leqslant xz)$ 直接得到。

利用保序性定理可直接证明以下定理。

定理 7.5 设$<A,\leqslant>$是格。对任意 $x,y,z\in A$，有

$$(x\leqslant y)\wedge(x\leqslant z)\Rightarrow(x\leqslant yz) \tag{7.7}$$

$$(x\leqslant y)\wedge(x\leqslant z)\Rightarrow(x\leqslant y\oplus z) \tag{7.8}$$

$$(x\geqslant y)\wedge(x\geqslant z)\Rightarrow(x\geqslant y\oplus z) \tag{7.9}$$

$$(x\geqslant y)\wedge(x\geqslant z)\Rightarrow(x\geqslant yz) \tag{7.10}$$

公式（7.9）与公式（7.7）及公式（7.10）与公式（7.8）两两是对偶的。

证明 证明式（7.7）。

设 $x\leqslant y$，$x\leqslant z$。则 x 是 y 和 z 的下界，而每一个下界都“小于等于”下确界，所以，$x\leqslant yz$。

证明公式（7.8）。从保序性定理可知，由于 $x\leqslant y$，故 $x\oplus x\leqslant x\oplus y$，即 $x\leqslant x\oplus y$；还因 $x\leqslant z$，故 $x\oplus y\leqslant y\oplus z$。结合这两个结果，同时考虑偏序关系是传递的就可得 $x\leqslant y\oplus z$。

定理 7.6 设$<A,\leqslant>$是格。对任意 $x,y,z\in A$，有

$$x\oplus(y\cdot z)\leqslant(x\oplus y)\cdot(x\oplus z) \tag{7.11}$$

$$x\cdot(y\oplus z)\geqslant x\cdot y\oplus x\cdot z \tag{7.12}$$

以上两式称为格上的**分配不等式**。

证明 由于有对偶原理，我们只需证明式（7.11）。

由运算“$\oplus$”的定义可知 $x\leqslant x\oplus y$ 和 $x\leqslant x\oplus z$。根据公式（7.7），得出 $x\leqslant(x\oplus y)\cdot(x\oplus z)$。

又因为 $yz\leqslant y\leqslant x\oplus y$ 和 $yz\leqslant z\leqslant x\oplus z$，得 $yz\leqslant(x\oplus y)\cdot(x\oplus z)$。最后从公式（7.9）可得

$$x\oplus(y\cdot z)\leqslant(x\oplus y)\cdot(x\oplus z)$$

定理 7.7 设$<A,\leqslant>$是格。对任意的 $x,y,z\in A$，有

$$x\leqslant z\Leftrightarrow(x\oplus yz\leqslant(x\oplus y)z) \tag{7.13}$$

这个公式又称为**模不等式。**

证明 因为 $x \leqslant z$，根据公式（7.5），有

$$x \oplus z = z$$

由于公式（7.11）对任何 $x, y, z \in A$ 都成立，所以，将那里的 $x \oplus z$ 置换为 z 就是公式（7.13）右边的式子。

反之，若式（7.13）右边不等式成立，可以看出 $x \leqslant x \oplus yz \leqslant (x \oplus y)z \leqslant z$，所以 $x \leqslant z$。

7.1.4 格与代数系统的对应

本节要引入一种叫做**代数格**的系统，它是偏序格的对应物或等价物。由于从代数系统的角度来研究格，所以代数系统的很多性质和运算规律可方便地引用至格上来。

定义 7.2 设 L 是非空集合，其上定义一个“加法”运算和一个“乘法”运算：“$\oplus$”和“$\cdot$”。并且满足式（7.2）、式（7.3）和式（7.4）表述的交换律、结合律和吸收律。代数系统$<L, \oplus, \cdot>$就称为**代数格**。代数格也简称格。

由于幂等律可以从以上几个定律导出，所以格代数是满足幂等律的。事实上，对任一个 $x \in L$，都有

$$xx = x(x \oplus xx) = x$$

当然，以上等式的对偶式 $x \oplus x = x$ 也是成立的。

下面就来证明本小节的主要内容：一个偏序格和一个代数格等价。

设$<L, \oplus, \cdot>$是一个代数格，构造 L 上的二元关系 R。对任意 $x, y \in R$，

$$xRy \Leftrightarrow (xy = x) \tag{7.14}$$

显然，对任意 $x \in L$，因为 $xx = x$，所以 xRx，R 是自反的。

若 $x, y \in L$，且 xRy, yRx。则按 R 的定义有 $xy = x$ 和 $yx = y$（或 $xy = y$），所以 $x = y$。R 是反对称的。

若 $x, y, z \in L$，且 xRy, yRz。则有 $xy = x$ 和 $yz = y$。那么 $xz = (xy)z = x(yz) = xy = x$。按照式（7.14）的定义，$xRz$。$R$ 是传递的。

证得 R 是 L 上的偏序关系。

由于 $xy = x$，所以 $x \oplus y = xy \oplus y = y$；反之，若 $x \oplus y = y$，则 $xy = x(x \oplus y) = x$。故 $xy = x$ 与 $x \oplus y = y$ 是等价的。因此，定义 R 的式子（7.14）也可写成

$$xRy \Leftrightarrow (x \oplus y = y) \tag{7.15}$$

还要证明偏序关系 R 还是一个偏序格。以下索性用“$\leqslant$”来代替“R”表示这个偏序关系。

由于代数格有吸收律，对任意 $x, y \in L, x \oplus xy = x$ 和 $y \oplus xy = y$。根据式（7.15）可得 $xy \leqslant x$ 和 $xy \leqslant y$。就是说 xy 是 x 和 y 的下界。若还有 $z \in L$ 也是 x 和 y 的下界，即 $z \leqslant x$ 和 $z \leqslant y$，就可知 $xz = z$ 和 $yz = z$。于是 $(xy)z = x(yz) = xz = z$，即 $z \leqslant xy$。这说明了 xy 是 x 和 y 的下确界。同样可证明 $x \oplus y$ 是 x 和 y 的上确界。即

$$\inf\{x, y\} = xy \qquad \sup\{x, y\} = x \oplus y \tag{7.16}$$

这样就证到了任一代数格$<L, \oplus, \cdot>$都与一个由式（7.14）或式（7.15）定义的偏序格对应。

另一方面，在本节偏序格的性质中已经阐明，若任意元素 $x, y \in L$（在那里，我们用$<A, \leqslant>$表示偏序格），按照式（7.16）定义了二元运算“$\oplus$”和“$\cdot$”，则等价式（7.5）就成立，并

且$\oplus$和$\bullet$运算满足交换律、结合律和吸收律。所以$<L,\oplus,\bullet>$是一个代数格。所以有：

定理 7.8 任何一个偏序格与一代数格等价。

格被定义成一种代数以后，我们有理由来考虑子格的概念。

定义 7.3 设$<L,\oplus,\bullet>$是一个格，$S\subseteq L$,S是L的子集。$<S,\oplus,\bullet>$是L的子格，当且仅当运算$\oplus$和$\bullet$在S上是封闭的。

从子格的定义可知，子格本身也是一个格。由于运算$\oplus$和$\bullet$不一定在格的每一个子集上都封闭，所以即使某一子集是一偏序格，但它不一定是子格*。

【例 7.3】 回过去看例 7.1 和图 7.2。$A=\{a,b,c\}$，就格$<\rho(A),\subseteq>$来说，子集$A_1=\{\{b\},\{a,b\},\{b,c\},\{a,b,c\}\}$,$A_2=\{\phi,\{a\},\{c\},\{a,c\}\}$和$A_3=\{\phi,\{a,b\},\{b,c\},\{a,b,c\}\}$对于包含关系“$\subseteq$”而言，$A_1,A_2,A_3$都是偏序格。但是只有$<A_1,\oplus,\bullet>$和$<A_2,\oplus,\bullet>$是$<A,\oplus,\bullet>$的子格，而$<A_3,\subseteq>$不是子格。因为$\{a,b\},\{b,c\}\in A_3$，但是$\{a,b\}\bullet\{b,c\}=\{b\}\notin A_3$。即运算$\bullet$在$A_3$上不封闭。

由这个例子，引出定理 7.8 的一个重要附注，就是偏序格与代数格的等价性，在子集或子代数层次上不必成立。说得明白些，即任何偏序格的子集所含的元素，若它们保持在原偏序格上的偏序关系，那么该子集连同它们之间的这个关系必然构成一个偏序集，有时甚至是一个偏序格*（如例 7.3 中的A_3）。但相应子代数格不一定同时存在。因为在子集上的某些元素对，它们在子集上的确界不同于它们在原先格中的确界。

【例 7.4】 设$\mathbf{Z}^+$是正整数集。D是$\mathbf{Z}^+$上的整除关系。即对任意$x,y\in\mathbf{Z}^+$，$xDy\Leftrightarrow x\mid y$。因为$x\cdot y$表示他们的最大公因数$\gcd(x,y)$，$x\oplus y$表示它们的最小公倍数$\mathrm{lcm}(x,y)$。所以$<Z^+,D>$是偏序格。

又设n表示某一正整数，$S_n\subseteq\mathbf{Z}^+$表示所有n的因数的集合。例如$n=8$，$S_8=\{1,2,4,8\}$。显然，$<S_8,D>$是一个偏序格，而且$<S_8,\oplus,\bullet>$同时还是$<\mathbf{Z}^+,\oplus,\bullet>$的子格。这个结论可以推广到$n$是任意正整数的情况。

7.2 有补格和分配格

格是附带某些特性的偏序集，有些特殊的格具有一些更进一步的特性。这些格最终引出我们的布尔代数。

设$<L,\oplus,\bullet>$是代数格，$<L,\leqslant>$是与之等价的偏序格。对任意$x,y\in L$，x,y有唯一的一个上确界和唯一的一个下确界。因此，可以通过数学归纳法证明，格的任何有限子集$S\subseteq L$，必有唯一的一个上确界和一个下确界。设$S=\{x_1,x_2,\cdots,x_n\}$，由于定理 7.2 之（3）的性质，即格上的运算$\oplus$和$\bullet$都满足结合律，所以，S的上确界和下确界可以表示成

$$\sup S=x_1\oplus x_2\oplus\cdots\oplus x_n$$

$$\inf S=x_1\bullet x_2\bullet\cdots\bullet x_n$$

一个格，若它的任何非空子集都有上、下确界，这样的格叫做**完备格**。显然，有限格一定是完备格。

若L是完备格，则L的上确界一定是它的最大元，L的下确界一定是L的最小元。我们以“1”和“0”分别表示一个**格的最大元**和**最小元**，并统称之为格L的**界**。

* 从第 3 章习题 3.38 的结果可知，偏序集的子集仍是偏序集，但是不一定是偏序格。

定义 7.4　一个含有最大元 1 和最小元 0 的格叫做**有界格**。

设<L,⊕, • >是有界格，那么，对任意 $x \in L$ 都有

$$0 \oplus x = x \quad 0 \cdot x = 0 \tag{7.17}$$

$$1 \cdot x = x \quad 1 \oplus x = 1 \tag{7.18}$$

这样，我们可以说 0 是加法⊕运算的么元，1 是乘法 • 运算的么元；0 同时也是乘法的零元，1 也是加法的零元（应该提醒读者的是，这里的 1 和 0 决不表示整数，它们各代表格的最大元和最小元）。

现在，尤其是给出了式（7.17）和式（7.18）两式之后，可以看出有界格的最大元 1 和最小元 0 是互相对偶的。因此，我们必须将定理 7.1（对偶原理）扩充到包含元素 0 和 1 的对换。

一般地，可以将有界格表示成<L, ⊕, • , 0, 1>。这是一个定义了两个二元运算和两个零元运算的特殊代数系统。

定义 7.5　设<L, ⊕, • , 0, 1>是有界格。若对 $x, y \in L$，有 $xy = 0$，$x \oplus y = 1$。则称 y 是 x 的**补元**，或 x是y 的补元。补元也简称为**补**。

定义 7.6　若一个有界格的每一元素都有补元，则称此有界格为**有补格**。

从补元的定义可知，这是一个对称的概念（因⊕、• 运算是可交换的），并且最大元 1 和最小元 0 是一对互补的元素：

$$0 \cdot 1 = 0 \qquad 0 \oplus 1 = 1 \tag{7.19}$$

对于一般的有界格而言，并非每一元素都有补元，或者，有些元素有不止一个补元。图 7.5 给出了这样的一些例。

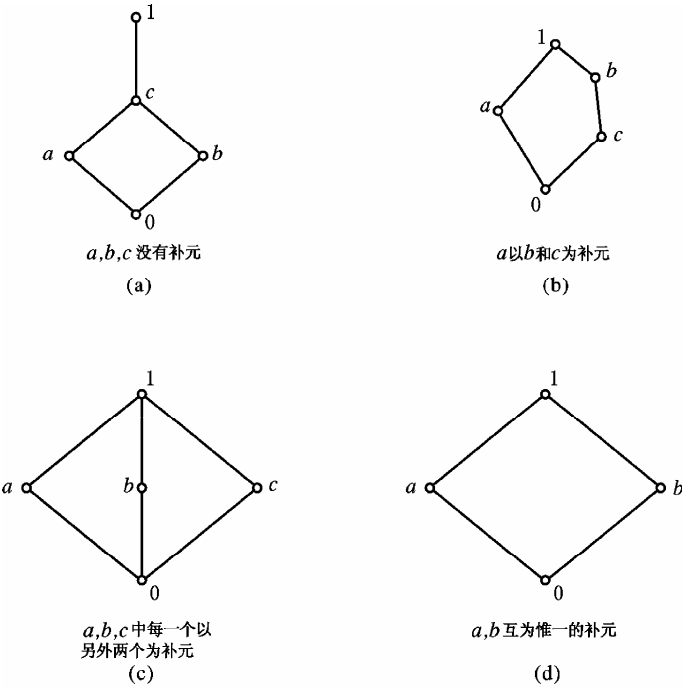


图 7.5　格的互补元

【例 7.5】　前一节的例 7.1 给出的幂集 $\rho(X)$ 上的格就是一个有补格。集合 ϕ 和 X 就是这个格的界。而且对任何 $A_i \in \rho(X)$，它的补是 $X - A_i$。所以<$\rho(X), \cup, \cap, \phi, X$ >是有补格。

【例 7.6】　前一节的例 7.2 给出了全体合式公式 F 上的格<$F, \Rightarrow$ >。公式 **T**（永真式）

和 **F**（永假式）是它的界。而且对任意合式公式公式 $f \in F$，否定式$\neg f$是它的补元。所以<F,$\vee$, $\wedge$,**F**,**T**>是有补格。

定义 7.7　其每一个二元运算对另一个都满足分配律的格<L,$\oplus$, $\cdot$>叫做**分配格**。即，对 $x,y,z \in L$，有

$$x \oplus (y \cdot z) = (x \oplus y) \cdot (x \oplus z) \tag{7.20}$$

$$x \cdot (y \oplus z) = x \cdot y + x \cdot z \tag{7.21}$$

其实，以上式（7.20）和式（7.21）两式并非都是独立的，因为它们是对偶的，因此，可从一个推出另一个。

现在回过去看例 7.5 和例 7.6 给出的两个格，它们各自的两个二元运算中任一个对另一个都满足分配律（分别参看第 3 章表 3.1 中的式（5）和第 2 章表 2.14 中的式（5））。所以这两个格都是分配格。

但有些格对其中某些元素可满足以上式（7.20）或式（7.21），而并不是对所有元素满足这两个公式。这样的格就不是分配格。以下是一个例子。

【例 7.7】　在图 7.5（b）给出的格中，虽然有

$$a(b \oplus c) = 0 \qquad ab \oplus ac = 0$$

$$c(a \oplus b) = c \qquad ca \oplus cb = c$$

但是

$$b(a \oplus c) = b \qquad ba \oplus bc = c$$

所以这不是分配格。

一般地说，验证某一具体的格是否是一个分配格需要对其所有可能的元素组合证实公式（7.20）或式（7.21）成立。而下面的定理可以使我们不必这样做就能做出判断。这个定理在理论上是重要的。

定理 7.9　任何全序集一定是分配格

证明　设<L,$\leqslant$>是全序集。它对应的代数格是<L,$\oplus$, $\cdot$>。由于对任意 $x,y,z \in L$，只能有以下两种可能：（1）$x \leqslant y$ 或 $x \leqslant z$，（2）$y \leqslant x$ 和 $z \leqslant x$。来证明在这每一种情况下公式（7.20）都成立。

就第一种情况，由于 L 是全序，所以，$y \oplus z = y$ 或 $y \oplus z = z$。无论如何总有

$$x(y \oplus z) = x$$

再考虑到第一种假设，$xy = x$ 或者 $xz = x$，最后，由吸收律又有

$$xy \oplus xz = x$$

就第二种情况，有

$$x(y \oplus z) = y \oplus z \qquad xy \oplus xz = y \oplus z$$

总之，分配律对<L,$\oplus$, $\cdot$>成立。

定理 7.10　设<L,$\oplus$, $\cdot$>是分配格。对任意 $x,y,z \in L$，有

$$xy = xz,\ \ x \oplus y = x \oplus z \Rightarrow y = z \tag{7.22}$$

证明

$$xy \oplus z = xz \oplus z = z$$

另一方面

$$xy \oplus z = (x \oplus z) \cdot (y \oplus z)$$

$$= (x \oplus y) \cdot (y \oplus z)$$
$$= y \oplus xz$$
$$= y \oplus xy = y$$

所以 $y = z$。

这个定理描述了分配格上的可约律。不过，它决不同于前一章里群上的可约律。因为若将格$<L,\oplus, \cdot>$析解为两个代数系统$<L,\oplus>$和$<L, \cdot>$的话，即使 L 是有界格，但 0，1 和 1，0 分别是运算“$\oplus$”和“$\cdot$”各自的幺元和零元。所以他们没有一个属于群（群是没有零元的）。但是，当这里的两个运算结合在一起并满足分配律的话，在前面式（7.22）给出的前提下（两个前提缺一不可），约去律成立。

7.3 布尔代数

布尔代数是一种特殊的代数格。

定义 7.8 一个格如果是有补格又是分配格，这样的格叫做**布尔代数**。

前一节已说明，每一个有补格的元素至少有一个补元。但是若这个有补格还是分配格，那么可证明每一元素有且只有一个补元。这样，元素 x 的补元就可记为 $\bar{x}$。

定理 7.11 布尔代数的每一元素有且仅有一个补元。

证明 设$<L,\oplus, \cdot, 0,1>$是布尔代数。对任意 $x \in L$，设 $\bar{x} \in L$ 是 x 的一个补元。若还有另一个补元 $\bar{x}_1$，来证 $\bar{x}_1 = \bar{x}$。

若不然，$\bar{x}_1 \neq \bar{x}$，由于 $\bar{x}_1$ 和 $\bar{x}$ 都是 x 的补元，所以

$$\bar{x}_1 x = 0 \qquad \bar{x}_1 \oplus x = 1$$
$$\bar{x} x = 0 \qquad \bar{x} \oplus x = 1$$

也即

$$\bar{x}_1 x = \bar{x} x \qquad \bar{x}_1 \oplus x = \bar{x} \oplus x$$

根据上节定理 7.10 得出 $\bar{x}_1 = \bar{x}$。矛盾。

元素 x 到它的补元 $\bar{x}$ 的映射称做**求补运算**。它是一个一元运算。所以布尔代数完整地可表达为$<L,\oplus, \cdot, \bar{}\ ,0,1>$，即布尔代数由一个非空子集 L 和两个二元运算“$\oplus$”，“$\cdot$”一个一元运算“$\bar{}$”以及两个零元运算“0”，“1”构成。

布尔代数是有补格，也是分配格。布尔代数具有格、有补格和分配格的一切性质。因此，布尔代数是具有诸多特性的代数系统，其中最主要的是以下两个：

1．布尔代数是一个对偶的代数系统，其上定义的两个二元运算“$\oplus$”和“$\cdot$”是对偶的；两个零元运算“0”和“1”是对偶的；一个自对偶的一元运算，即补运算。

2．布尔代数作为一个格，隐含某一偏序集作为它的对应物。这个偏序集可由本章式（7.14）或式（7.15）给出。

有时，一个代数系统往往与一个关系有着密切地联系（第 6 章 6.8 节讨论过的代数系统上的同余关系就是如此）。这样的关系，通常揭示了代数系统本身种种重要的特征。

现在，我们从应用的角度来归纳布尔代数的种种性质。因为这里并非是在建立布尔代数

的**公理系统**[*]，所以，将要给出的有些性质并不是独立的，也即有些性质可以从另一些性质中导出。

设$<B,\oplus,\cdot,\bar{},0,1>$是一个布尔代数。对任意$x,y,z\in B$有以下性质：

1．满足格的所有性质。

$$xx=x \qquad x\oplus x=x$$
$$xy=yx \qquad x\oplus y=y\oplus x$$
$$(xy)z=x(yz) \qquad (x\oplus y)\oplus z=x\oplus(y\oplus z)$$
$$x(x\oplus y)=x \qquad x\oplus xy=x$$

2．满足有界格的所有性质。

$$0\leqslant x\leqslant 1$$
$$0\cdot x=0 \qquad 1\oplus x=1$$
$$1\cdot x=x \qquad 0\oplus x=x$$

3．满足有补格和分配格的所有性质。

$$x\cdot\bar{x}=0 \qquad x\oplus\bar{x}=1$$
$$\bar{0}=1 \qquad \bar{1}=0$$
$$x\oplus(y\cdot z)=(x\oplus y)\cdot(x\oplus z) \qquad x\cdot(y\oplus z)=x\cdot y\oplus x\cdot z$$
$$\overline{(xy)}=\bar{x}\oplus\bar{y} \qquad \overline{(x\oplus y)}=\bar{x}\cdot\bar{y}$$

以上最后这两个公式也叫做**摩根律**（De Morgen）。

4．通过公式（7.14）或公式（7.15）定义的偏序集$<B,\leqslant>$是布尔代数B的对应物，并且

$$xy=\inf\{x,y\} \qquad x\oplus y=\sup\{x,y\}$$
$$(x\leqslant y)\Leftrightarrow(xy=x) \quad (y\leqslant x)\Leftrightarrow(x\oplus y=x)\ ^{**}$$
$$(x\leqslant y)\Leftrightarrow(x\bar{y}=0) \quad (y\leqslant x)\Leftrightarrow(x\oplus\bar{y}=1)\ ^{**}$$
$$(x\leqslant y)\Leftrightarrow\bar{y}\leqslant\bar{x}$$

关于摩根律的证明，可以通过直接运算$(xy)\cdot(\bar{x}\oplus\bar{y})=0$和$(xy)\oplus(\bar{x}\oplus\bar{y})=1$验证。至于性质4的最后两行上的等价式留做习题，由读者完成。

以下是几个关于布尔代数的例子。

【例 7.8】 集合$B=\{0,1\}$，定义二元运算“$\oplus$”和“$\cdot$”及一元运算“$\bar{}$”，如表7.1给出。代数系统$<B,\oplus,\cdot,\bar{},0,1>$满足布尔代数的一切性质。这是一个二元布尔代数，也是最简单的布尔代数。可是它却有着广泛的应用。

表 7.1

$\cdot$	0	1	$\oplus$	0	1	x	$\bar{x}$
0	0	0	0	0	1	0	1
1	0	1	1	1	1	1	0

【例 7.9】 B_n是以0和1为分量的n元一维向量的集合（例如$b=(\underbrace{0,0,0,\cdots,0}_{n个})\in B_n$）。在$B_n$

[*] 一个公理系统要具有一致性、完备性和独立性。

** 这两个公式呈现这样的形式是考虑到对偶性的直观。读者可以自行将其中的x和y对调，以得到我们习惯的样子。如第二个可以表示成$(x\leqslant y)\Leftrightarrow(\bar{x}\oplus y=1)$。

上定义两个二元运算“按分量的和”运算“$\oplus$”和“按分量的乘”运算“$\cdot$”以及一元运算“按分量的取非（补）”的运算“$\bar{}$”。定义如下：

对任意 $x=(x_1,x_2,\cdots,x_n)\in B_n$，$y=(y_1,y_2,\cdots,y_n)\in B_n$

$$x\cdot y=(x_1\wedge y_1,x_2\wedge y_2,\cdots,x_n\wedge y_n) \tag{7.23}$$

$$x\oplus y=(x_1\vee y_1,x_2\vee y_2,\cdots x_n\vee y_n) \tag{7.24}$$

$$\bar{x}=(\neg x_1,\neg x_2,\cdots,\neg x_n) \tag{7.25}$$

其中运算“$\wedge$”，“$\vee$”，“$\neg$”是通常的逻辑运算合取：析取和非。于是代数系统$<B_n,\oplus,\cdot,\bar{},0_n,1_n>$构成布尔代数。其中 $0_n=(\underbrace{0,0,\cdots,0}_{n个})$ 是相对于运算$\oplus$的么元，$1_n=(\underbrace{1,1,\cdots,1}_{n个})$ 是相对于运算$\cdot$的么元。这个代数系统也叫做**开关代数**。

【例 7.10】 在 7.2 节例 7.5 中提到的格所对应的代数$<\rho(X),\cup,\cap,\sim,\phi,X>$，也是布尔代数。其中，“$\sim$”是集合的补集运算。元素$\phi$和$X$分别是最小元和最大元。这是一个**集合代数**。

【例 7.11】 在 7.2 节例 7.6 提到的合式公式的集F上的格所对应的代数$<F,\vee,\wedge,\neg,0,1>$是布尔代数。其中 0 和 1 各表示永假式和永真式。0 是系统的最小元，1 是最大元。这是一个**命题代数**。

若将集合限制在恰有n个命题变元的公式上，并以F_n表示这些公式的集合，则代数$<F_n,\vee,\wedge,\neg,0,1>$是以上命题代数的子布尔代数。

7.4 布尔表达式

到现在为止，我们讨论的都是一个布尔代数上的元素所满足的种种规律。可以把一个布尔代数$<B,\oplus,\cdot,\bar{},0,1>$上的所有元素看成是“常量”，而本节要讨论的是一些含有变量的表达式。这些表达式由一些字母（变量）和代数B上定义的运算以及括号按一定的规则组成，且每一变量在必要时可以且仅可以用布尔代数B的元素来取代。有趣的是，由布尔表达式又可构成一个新的布尔代数。这种由布尔表达式引出的代数又叫做自由布尔代数。再通过引入布尔表达等价的概念，讨论它的主范式。最后用布尔表达式来定义布尔函数。

设$x_1,x_2,\cdots,x_n$是n个字母（或变量，或变元）。

定义 7.9 含n个变元$x_1,x_2,\cdots,x_n$的，有限次引用以下规则生成的符号串叫做**合式的布尔表达式**，或简称为**布尔表达式**。

1．0 和 1 是布尔表达式。

2．每一个变元$x_1,x_2,\cdots,x_n$是布尔表达式。

3．若α,β是布尔表达式，则$(\alpha\oplus\beta),(\alpha\cdot\beta)$是布尔表达式。

4．若α是布尔表达式，则$\bar{\alpha}$是布尔表达式。

5．一个有限次运用上述四步骤生成的符号串是布尔表达式。

以后，我们用希腊字母α,β,γ等表示一个布尔表达式，或者将它包含的变元一并列表，表示成如$\alpha(x_1,x_2,\cdots,x_n)$的样子。

下面是一些布尔表达式的例子

$$x_1\oplus x_2,\ x_3,\ x_1\cdot x_2,\ x_1\oplus x_2\cdot x_3,\cdots$$

从形式上看，由n个变元组成的布尔表达式有无限多个。可是，类似于命题公式中的合

式公式那样，本质上，无限个布尔表达式实际上仅仅分别属于有限个子类，而每一子类中的表达式在某种意义下是等价的。

定义 7.10 两个布尔表达式$\alpha(x_1,x_2,\cdots,x_n)$和$\beta(x_1,x_2,\cdots,x_n)$是**等价**（相等）的，当且仅当有限次利用布尔代数所满足的恒等式，可将其中一个表达式化做另一个。

若布尔表达式α与β等价，则记为$\alpha=\beta$。

根据第 3 章 3.3 节等价关系的性质，我们可以将所有（n元）布尔表达式的每一个，归类到相应的一个等价类中去。

下面将要证明，n元布尔表达式上的等价关系诱导的等价类总共有2^{2^n}个。

定义 7.11 由所有n个变元$x_1,x_2,\cdots,x_n$或者它们的补元的积组成的表达式

$$\tilde{x}_1\cdot\tilde{x}_2\cdot\ldots\cdot\tilde{x}_n$$

称为一个**小项**。其中$\tilde{x}_i$不是x_i本身，就是其补元$\bar{x}_i$。

小项也叫**完全积**。

在第 2 章 2.6 节中，关于合式公式小项的编码规则同样适用于此。如 n=2，则共有 4 个小项，它们是

$$m_0=m_{00}=\bar{x}_1\cdot\bar{x}_2 \qquad m_1=m_{01}=\bar{x}_1\cdot x_2$$
$$m_2=m_{10}=x_1\cdot\bar{x}_2 \qquad m_3=m_{11}=x_1\cdot x_2$$

可以证明，关于小项有以下性质

$$m_i\cdot m_j=0 \qquad \text{当}\ i\neq j \tag{7.26}$$

$$m_0\oplus m_1\oplus\cdots\oplus m_{2^n-1}=1^* \tag{7.27}$$

即不同小项的积恒为 0，所有2^n个小项的和恒为 1。由于式（7.26）至少同时包含一个变元和这个变元的补元，所以它等于 0。对于式（7.27），可以对n用归纳法证明（参阅电子课件第 7 章 7.4 节）。严格地说，小项本身并没有确定的值，在这里，我们假定小项中n个变元均已被任一布尔代数$<B,\oplus,\cdot,\bar{}>$中的任意n个元素一一代入，并且运算满足本章 7.3 节关于布尔代数的恒等式。

运用第 2 章 2.6 节同样的方法可以证明，任一个含有n个变元的布尔表达式（表达式 0 除外），均可利用布尔代数的恒等式化做与之等价的若干不相同的小项之和。并且，如果不计变元在小项中的次序，也不计各小项的先后次序（因为布尔代数满足交换律和结合律，所以这些次序是非本质的），这样得到的各小项和的表达式是唯一的，并称之为n元布尔表达式的**主积和范式**。所以可以说两个等价的 n 元布尔表达式有相同的主积和范式。

【例 7.12】 将下列布尔表达式化做含x_1,x_2,x_3的等价的主积和范式：

（1）$\bar{x}_1\bar{x}_2$

（2）$x_1\oplus\bar{x}_2$

（3）$(\overline{\bar{x}_1\oplus x_2})\bar{x}_3$

解

（1）$\bar{x}_1\bar{x}_2=\bar{x}_1\bar{x}_2\ (x_3\oplus\bar{x}_3)=\bar{x}_1\bar{x}_2\,\bar{x}_3\oplus\bar{x}_1\bar{x}_2x_3$

（2）$x_1\oplus\bar{x}_2=x_1(\bar{x}_2\oplus x_2)\oplus\bar{x}_2(\bar{x}_1\oplus x_1)$

$=x_1\bar{x}_2\oplus x_1x_2\oplus\bar{x}_1\bar{x}_2\oplus x_1\bar{x}_2$

---

* 参考课件中相应的章节。

$$= x_1\bar{x}_2(\bar{x}_3 \oplus x_3) \oplus x_1x_2(\bar{x}_3 + x_3) \oplus \bar{x}_1\bar{x}_2(\bar{x}_3 \oplus x_3)$$
$$= \bar{x}_1\bar{x}_2\bar{x}_3 \oplus \bar{x}_1\bar{x}_2x_3 \oplus x_1\bar{x}_2\bar{x}_3 \oplus x_1\bar{x}_2x_3 \oplus x_1x_2\bar{x}_3 \oplus x_1x_2x_3$$

（3）$(\overline{\bar{x}_1 \oplus x_2})\bar{x}_3 = x_1\bar{x}_2\ \bar{x}_3$

由于含 n 个变元的布尔表达式共有 2^n 个不同的小项，所以如果包含 0 这个特殊的主积和范式在内，则共有 2^{2^n} 个不同的主积和范式。因为一个 n 元布尔表达式总是与唯一的一个主积和范式等价，否则就与 0 等价。所以，由 n 元布尔表达式等价关系诱导的等价类一共有 2^{2^n} 个。

运用对偶的概念可以给出大项和**主和积范式**的概念。不再赘述。

以下，我们来建立自由布尔代数的概念。为此先做一些准备工作。暂时从布尔表达式转到布尔代数的讨论上来。

定义 7.12　设$<B,\oplus,\bullet,\bar{}>$是布尔代数。对元素 $x \in B$，若并不存 $y \in B$ 且 $y \neq x$，满足 $y \leqslant x$ 和 $y \neq 0$（或者换一种说法是：对任意 $y \in B$ 且 $y \neq x$，如果 $y \leqslant x$，则有 $y = 0$），则 x 称为一个**原子元素**，简称**原子**（其中“≤”是该布尔代数对应的偏序格）。

定义 7.13　设 $<L,\oplus,\cdot>$ 是格，如果元素 $a \in L$，不能被表示成 L 中两个不同于 a 的元素的和，则称元素 a 是**和不可约**的。即，若 $a_1, a_2 \in L$，则

$$(a = a_1 \oplus a_2) \Rightarrow (a_1 = a \text{或} a_2 = a) \qquad (7.28)$$

可以证明，在布尔代数上，除元素 0 和原子是和不可约的之外，其他每一元素均可唯一地被表示成若干不同原子的和*。图 7.6 给出了有 2^1 个、2^2 个和 2^3 个元素的布尔代数。其中图 7.6（a）除下界 0 之外的另一个元素本身就是原子。图 7.6（b）中有两个原子 a,b。图 7.6（c）有 3 个原子 a,b,c。并且图 7.6（b），图 7.6（c）中的每一非零、非原子的元素都表示成了各自系统中若干原子之和。

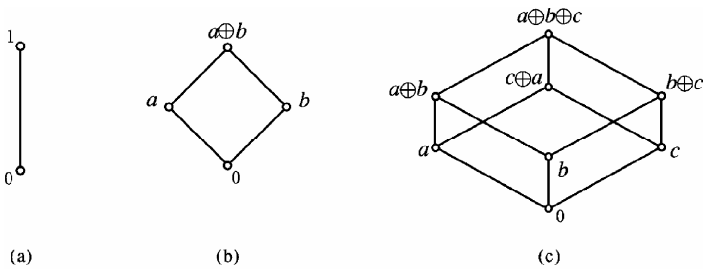


图 7.6 布尔代数上的原子

现在来看一个有 n 个原子的布尔代数 $<B,\oplus,\bullet,\bar{},0,1>$。$A = \{a_1, a_2, \cdots, a_n\}$ 是 B 的 n 个原子的集。于是我们可以建立一个 B 上的每一元素和 A 的子集之间的一一对应关系：下界 0 对应空集 ϕ，每一原子 a_i 对应 $\{a_i\}$。其他每一元素因为均可唯一地表示成若干原子之和的结果，如 $b \in B$，$b = a_{i_1} \oplus a_{i_2} \oplus \cdots \oplus a_{i_k}$，则元素 b 对应子集 $\{a_{i_1}, a_{i_2}, \cdots, a_{i_k}\}$。反之，由 A 的任一子集 A_b 中所有原子之和必然等于 B 中某一元素 $b \in B$。这样，上述一一对应就确切地建立了起来。而有 n 个原子的集 A 共有 2^n 个不同的子集，所以布尔代数 B 恰有 2^n 个不同的元素。

现在可以说：任何一个有限布尔代数所含有的元素个数，一定是 2^n 个（n 是有限布尔代数原子的个数，$n \geqslant 1$）。

---

* 参阅书末所列的参考文献之 5。

定义 7.14 设$<B,\oplus,\cdot,\bar{},0,1>$和$<P,\cup,\cap,\sim,\alpha,\beta>$是两个布尔代数。若映射 $f:B\to P$ 保持布尔代数上所有 5 种运算关系，也即对任意 $x,y\in B$，有

$$f(x\oplus y)=f(x)\cup f(y)$$
$$f(x\cdot y)=f(x)\cap f(y)$$
$$f(\bar{x})=\sim f(x)$$
$$f(0)=\alpha$$
$$f(1)=\beta$$

其中 $\sim f(x)$ 表示 $f(x)$ 在 P 中的补元。那么称 f 是 B 到 P 的一个**布尔同态**。又若 f 是双射，则 f 就是 B 到 P 的一个**布尔同构**。

基于上述有 n 个原子的布尔代数所有元素与这些原子组成的全部子集一一对应的关系，我们可以建立一个布尔代数 B_n 到 $\rho(A)$（A 是该布尔代数全部原子的集合）的映射：$f:B_n\to\rho(A)$，并且通过逐一验证它满足定义 7.14 所列的 5 个等式。于是，有如下的**布尔代数的表示定理**。

定理 7.12 （Stone 表示定理）设$<B_n,\oplus,\cdot,\bar{},0,1>$是一有限布尔代数。$A$ 是此布尔代数所有 n个 原子的集。则$<B_n,\oplus,\cdot,\bar{},0,1>$与集合代数$<\rho(A),\cup,\cap,\sim,\phi,A>$同构。

现在回到布尔表达式的讨论上去。由公式（7.26）和公式（7.27）可以看出，n 元布尔表达式的小项具有布尔代数上原子的性质。以 S 表示这所有 2^n 个小项的集合，根据定理 7.12 和以上的讨论，集合代数$<\rho(S),\cup,\cap,\sim,\phi,S>$和一个以 n 元布尔代数的 2^n 个小项为原子的布尔代数$<B_n,\oplus,\cdot,\bar{},0,1>$是同构的。在此，元素 0 对应 ϕ，1 对应 S（对应所有小项的和）。而其余每一个 n 元布尔表达式 $b\in B_n$，对应于 S 的一个真子集，它包含表达式 b 的主积和范式里的所有小项。我们称这个由一切 n 元布尔表达式（等价的表达式视为一个，并以主积和范式作为代表）组成的布尔代数为**自由布尔代数**。这就是说，n 元自由布尔代数含有 2^{2^n} 个元素*。

一个 n 元的布尔表达式本身并无任何值。但是，如果以任一个布尔代数$<B,\oplus,\cdot,\bar{}>$的 n 个元素一一代替表达式中的每一变元之后，该表达式最后取布尔代数 B 上的某一元素作为它的值。这方面和一个代数表达式 $x^3+3x^2y+5xy^2+6y^3$ 在实数集上通过用实数代换其中变元 x,y 而最后有实数值一样。这个事实提示人们，可用一个布尔表达式“解析地”在任意一个布尔代数的集合 B 上定义一个函数。我们称这种函数为**布尔函数**。

设$<B,\oplus,\cdot,\bar{},0,1>$是任意布尔代数。$\alpha(x_1,x_2,\cdots,x_n)$ 是布尔表达式，而 $\alpha(a_1,a_2,\cdots,a_n)$ 表示用集合 B 的笛卡尔积 B^n 上的一个 n 元组$<a_1,a_2,\cdots,a_n>$的每一个元素逐一取代布尔表达式 α 的每一个变元 $x_1,x_2,\cdots,x_n$ 后的布尔表达式。显然 $\alpha(a_1,a_2,\cdots,a_n)\in B$。就是说 $\alpha(a_1,a_2,\cdots,a_n)$ 是布尔代数$<B,\oplus,\cdot,\bar{},0,1>$的一个元素。

若 $\alpha(x_1,x_2,\cdots,x_n)$ 和 $\beta(x_1,x_2,\cdots,x_n)$ 是两个在定义 7.10 的意义下相等的布尔函数。对任意布尔代数 B，以 B^n 的 n 元组$<a_1,a_2,\cdots,a_n>$同时对 α,β 赋值，就有两个布尔代数 B 上的算式 $\alpha(a_1,a_2,\cdots,a_n)$ 和 $\beta(a_1,a_2,\cdots,a_n)$。既然 α 与 β 是等价的，因此，可以有限次地应用布尔

* 其中只有元素 0 不能被表示为小项的和，它对应到空集 ϕ。

代数的恒等式对其中一个（如 $\alpha(a_1,a_2,\cdots,a_n)$ ）进行变换而最终得到另一个。这说明 $\alpha(a_1,a_2,\cdots,a_n)=\beta(a_1,a_2,\cdots,a_n)$。于是我们有以下重要的结论：

定理 7.13 以任意一个布尔代数的元素同时给两个等价（相等）的布尔表达式以相同赋值，其结果是这两个布尔表达式有相同的值。

对一个布尔表达式以二元布尔代数<{0,1},⊕, •, $\bar{}$ >的元素赋值叫做**二元赋值**。二元赋值有着特殊的、重要的意义。事实上，7.3 节的例 7.11 所提到的命题代数<*F*,∨,∧,¬ ,0,1>就是一个自由布尔代数。每一合式公式 $f\in F$ 是一布尔表达式，我们记得（在第 2 章 2.2.2 小节），条件“→”和双条件“⇄”都可以用“¬ ”和“∨”或“∧”化去，对合式公式的每一次赋值都是二元赋值。

现在，我们要用二元赋值来说明定理 7.13 的逆同样成立。

我们来讨论用二元布尔代数上仅有的两个元素 0 和 1 对所有 *n* 元布尔表达式赋值。类似于第 2 章 2.6.1 小节的讨论，我们有理由说，对一个 *n* 元布尔表达式的小项施二元赋值，并使该小项的值为 1，当且仅当这组赋值恰与该小项的二进制编码相等。并且，一个 *n* 元布尔表达式的主积和范式（如果该布尔表达式不是 0）恰恰等于某些小项之和，这些小项的编码是与使布尔表达式的值为 1 的各组赋值一一对应的。因此，若有两个 *n* 元布尔表达式在每一次二元赋值下都有相等的值，那么这两个 *n* 元布尔表达式必有相同的主积和范式。于是这两个布尔表达式是等价（相等）的。

归纳以上的讨论，我们已经得到的结论是这样的：

1. 对两个等价的布尔表达式在任意布尔代数下的每一次相同的赋值都使这两个布尔表达式的值相等。

2. 对两个布尔表达式所做的每一次相同的二元赋值都使两布尔表达式取相等的值，那么该两布尔表达式等价。

3. 两布尔表达式在某一确定的布尔代数下的每一次相同赋值都有相等的值，则这两个布尔表达式是等价的。

定理 7.14 若以某一确定的布尔代数上的元素对两个布尔表达式的每一次相同赋值，都使两布尔表达式取同样的值，那么这两个布尔表达式是等价（相等）的。

该定理也同样可以作为两布尔表达式等价（相等）的定义。

【例 7.13】 证明以下三元布尔表达式两两是等价的。

（1） $\bar{x}_1x_2\oplus\bar{x}_3$

（2） $\overline{(x_1\oplus\bar{x}_2)x_3}\oplus x_1\bar{x}_3$

（3） $(\bar{x}_1\oplus\bar{x}_3)(x_1\oplus x_2)(x_2\oplus\bar{x}_3)\oplus\bar{x}_3$

解 因为以上式（2）

$$\begin{aligned}&\overline{(x_1\oplus\bar{x}_2)x_3}\oplus x_1\bar{x}_3\\=&\overline{(x_1\oplus\bar{x}_2)}\oplus\bar{x}_3\oplus x_1\bar{x}_3\\=&\bar{x}_1x_2\oplus\bar{x}_3\end{aligned}$$

这样就证明了（2）与（1）等价。

此外，式（3）

$$
\begin{aligned}
&(\bar{x}_1 \oplus \bar{x}_3)(x_1 \oplus x_2)(x_2 \oplus \bar{x}_3) \oplus \bar{x}_3 \\
&= (\bar{x}_1 x_2 \oplus x_1 \bar{x}_3 \oplus x_2 \bar{x}_3)(x_2 \oplus \bar{x}_3) \oplus \bar{x}_3 \\
&= \bar{x}_1 x_2 \oplus x_1 x_2 \bar{x}_3 \oplus x_2 \bar{x}_3 \oplus \bar{x}_1 x_2 \bar{x}_3 \oplus x_1 \bar{x}_3 \oplus x_2 \bar{x}_3 \oplus \bar{x}_3 \\
&= \bar{x}_1 x_2 \oplus \bar{x}_3
\end{aligned}
$$

所以式（3）与（2）等价，最后（1），（2），（3）两两等价。

以上等式最后一步自右至左连续 5 次使用了吸收律。

下面的表 7.2 是以上各表达式在二元赋值下的值，可见在每一组二元赋值下它们的值都是相同的。

表 7.2

x_1	x_2	x_3	$\bar{x}_1 x_2$	式（1）	$x_1 \oplus \bar{x}_2$	$(x_1 \oplus \bar{x}_2)x_3$	$x_1 \bar{x}_3$	式（2）	$x_1 \oplus x_2$	$\bar{x}_1 \oplus \bar{x}_3$	$x_2 \oplus \bar{x}_3$	式（3）
0	0	0	0	1	1	0	0	1	0	1	1	1
0	0	1	0	0	1	1	0	0	0	1	0	0
0	1	0	1	1	0	0	0	1	1	1	1	1
0	1	1	1	1	0	0	0	1	1	1	1	1
1	0	0	0	1	1	0	1	1	1	1	1	1
1	0	1	0	0	1	1	0	0	1	0	0	0
1	1	0	0	1	1	1	1	1	1	1	1	1
1	1	1	0	0	1	1	0	0	1	0	1	0

设$<B, \oplus, \cdot, \bar{}, 0, 1>$是一个布尔代数。由于对一个 n 元布尔表达式 $\alpha(x_1, x_2, \cdots, x_n)$ 在布尔代数 B 上的每一个 n 元赋值，表达式 α 都有一确定的值。因此，一个 n 元布尔表达式定义了一个 $B^n \to B$ 的函数。

定义 7.15 $<B, \oplus, \cdot, \bar{}>$是一个布尔代数。由一个 n 元布尔表达式定义的 $B^n \to B$ 上的函数叫做**布尔函数**。

前面已经讲过，n 元布尔表达式构成的自由布尔代数含有 2^n 个小项，并且小项都是原子。因此，n 元布尔表达式的自由布尔代数共含有 2^{2^n} 个不等价的布尔表达式。也就是说任何一个布尔代数上定义的 n 元布尔函数有且仅有 2^{2^n} 个。设一个布尔代数含有 m（$m = 2^i$，i 为布尔代数的原子的数目）个元素，即 $|B| = m$。从第 3 章 3.5.1 小节的讨论可知，所有 $B^n \to B$ 的 n 元函数的集合可以记为 B^{B^n}，并且该集合包含 m^{m^n} 个 n 元函数。当 $m = 2$ 时，那么定义在二元布尔代数上的 n 元布尔函数的数目恰好等于定义在它上面的所有 n 元函数的数目，2^{2^n} 个。也就是说，任何定义在二元布尔代数上的 n 元函数都是一个 n 元布尔函数，即每一个这样的 n 元函数都可以被解析地表达。但是，当 $m > 2$ 时，通过计算表明，n 元函数的数目就要多于 n 元布尔函数。换句话说，在 $m > 2$ 时，m 元布尔代数上的很多 n 元函数是不能由 n 元布尔表达式来解析地定义的。恐怕这也是通常我们舍弃多值逻辑而更倾向于二值逻辑的一个很重要的原因吧。下面是一个例子。

【例 7.14】 设$<B, \oplus, \cdot, \bar{}, 0, 1>$是 4 元布尔代数。$B = \{a, b, 0, 1\}$。图 7.6（b）给出了相应的图（在那里 $a \oplus b = 1$ 是最大元）。试写出所有 $B^2 \to B$ 的二元布尔函数，并举一例说明某一个 $B^2 \to B$ 的二元函数并不是布尔函数（它不能被解析地表示成二元布尔函数）。

解 设 $B^2 \to B$ 的二元函数的集合是 F，则 $|F| = 4^{4^2}$，即共有 4 294 967 296 个二元函数。

但 $B^2 \to B$ 的布尔函数仅有 $2^{2^2}=16$ 个。这 16 个布尔函数组成了二元自由布尔代数。我们可以通过它的 4 个原子，也即 4 个小项的不同组合用主积和范式给出：

$$b_0(x,y)=0 \qquad b_1(x,y)=\bar{x}\cdot\bar{y}$$
$$b_2(x,y)=\bar{x}y \qquad b_3(x,y)=x\bar{y}$$
$$b_4(x,y)=xy \qquad b_5(x,y)=\bar{x}\cdot\bar{y}\oplus\bar{x}y$$
$$b_6(x,y)=\bar{x}\cdot\bar{y}\oplus x\bar{y} \qquad b_7(x,y)=\bar{x}\cdot\bar{y}\oplus xy$$
$$b_8(x,y)=\bar{x}y\oplus x\bar{y} \qquad b_9(x,y)=\bar{x}y\oplus xy$$
$$b_{10}(x,y)=x\bar{y}\oplus xy \qquad b_{11}(x,y)=\bar{x}\cdot\bar{y}\oplus\bar{x}y\oplus x\bar{y}$$
$$b_{12}(x,y)=\bar{x}\cdot\bar{y}\oplus\bar{x}y\oplus xy \qquad b_{13}(x,y)=\bar{x}\cdot\bar{y}\oplus x\bar{y}\oplus xy$$
$$b_{14}(x,y)=\bar{x}y\oplus x\bar{y}\oplus xy \qquad b_{15}(x,y)=\bar{x}\cdot\bar{y}\oplus\bar{x}y\oplus x\bar{y}\oplus xy$$

以上这些布尔函数都用范式表示，并不一定是最简单的形式。例如，b_{15} 可化简成 $b_{15}=1$。

最后，我们来定义一个不同于以上 16 个布尔函数的二元函数。

实际上一个 $B^2 \to B$ 的二元函数 $f(x,y)$，对定义域 B^2 的 16 个不同的序偶（自变量），每一个指定一个函数值 $f(x,y)$，使之逐一不同于以上 16 个布尔函数在相同自变量下的值。例如，当 $<x,y>=<0,0>$，$b_0(0,0)=0$；但令 $f(0,0)=1\neq 0$，$b_1(0,a)=b$；但令 $f(0,a)=a\neq b$，$b_2(0,b)=b$；但令 $f(0,b)=a\neq b$ 等等。这总是可以做到的。显然，$f(x,y)$ 不等于以上 16 个布尔函数中任何一个。注意到，用类似的方法，我们可以得到 4 294 967 280 个不属于布尔函数的二元函数。

【例 7.15】 命题演算可以用二元布尔代数<{0,1}∨,∧,¬,0,1>来描述，其中 0 和 1 是命题的两个真值。一个有 n 个命题变元的命题公式 $f(x_1,x_2,\cdots,x_n)$ 是一个布尔表达式。每一个由 $\{0,1\}^n \to \{0,1\}$ 的 n 元函数都可以用一个合式公式表示。因为在二元布尔代数上这样的 n 元函数一共有 2^{2^n} 个，而这也是所有 n 元布尔函数的数目。即所有定义在二元布尔代数<{0,1},∨,∧,¬,0,1>上的 n 元函数都是 n 元布尔函数（合式公式）。

【例 7.16】 设 A 是一个非空集合，$|A|=m$。集合代数<$\rho(A)$,∪,∩,～,ϕ,A>是一个布尔代数。考虑此集合代数上的 n 元布尔表达式 $\alpha(x_1,x_2,\cdots,x_n)$，可知共有 2^n 个小项，因此以此 2^n 个小项为原子的自由布尔代数<B,∪,∩,～,ϕ,A>共有 2^{2^n} 个布尔表达式或布尔函数。当 $m>1$，或 $|\rho(A)|>2$ 时，就会出现定义在 $(\rho(A))^n \to \rho(A)$ 的，并且不能表达成布尔表达式的集合函数。

7.5 布尔函数的表示及极小化

在第 2 章 2.8 节中，我们已经讨论过二值逻辑电路的简单设计问题。现在可以说，一个有一位输出有 n 位输入的逻辑电路，对应数学上的一个 n 元布尔函数 $p=f(x_1,x_2,\cdots,x_n)$。由于目前几乎所有逻辑电路都是二值的，所以，我们仅讨论定义在 $\{0,1\}^n \to \{0,1\}$ 的布尔函数。换一个角度说，每一个 n 元布尔函数，对应一个有 n 位输入端和一位输出端的逻辑电路。而布尔函数中的运算“⊕”（或）、“·”（与）和“¯”（非）各对应电路中的一个“或门”、“与门”和“反相器”等器件。显然，将一个布尔函数按某种标准极小化，可以在不改变一个逻辑电路功能的前提下，减少组成电路的器件数目，降低成本或提高电路反应速度。而要极小

化一个布尔函数，首先要建立一些便于做极小化计算的布尔函数的表示法。本节首先讨论布尔函数的种种表示法，然后简要地介绍一些极小化方法。

7.5.1 布尔函数的表示法

以下各种布尔函数的表示，各适用不同的极小化方法。

上一节已经说过，一个 n 元布尔函数可以用一个合式的 n 元布尔表达式解析定义。用布尔表达式的好处在于可以用布尔代数的恒等式方便地化简布尔函数。这是布尔函数的第一种表示法。这方面，可参考第 2 章 2.8 节中的一些例子。

第二种表示布尔函数的方法是**表格法**，即将所有可能的输入组合和相应的输出结果列在一张表中。一个布尔函数的表格类似本章 7.4 节的表 7.2。表格法的好处是明确直观，对给定的一组输入，查表可立刻得到相应的输出。但用表格表示的布尔函数不适用化简工作，而且当输入变元超过 4～5 个时，表格会变得很庞大。表格行的数目会随输入端的增加成几何级数的增长。

另一种布尔函数的表示法是 n **维空间图示法**。首先为 n 元布尔函数的输入预先约定一个次序，如 $\{x_1, x_2, \cdots, x_n\}$。然后，按某种下面将要阐明的规则，将这 2^n 组不同的输入分别排列在一个 n 维立方体的各顶点上。并且，输出为 1 对应的输入 n 元组，用一个小圆点画出，对应输出为 0 的 n 元组则不画小圆点。

为了说明这些输入的 n 元组是如何排列在 n 维立方体上的，先来看以下定义。

定义 7.16　两个 n 元组 $(x_1, x_2, \cdots, x_n)$ 和 $(y_1, y_2, \cdots, y_n)$ 的每一分量 x_i，y_i 只取 0 或 1 两个值，它们的距离就是所有不相等分量的数目。这样定义的距离也叫**海明**（Hamming）**距离**。

图 7.7 是一个 3 维立方体。对应的 $2^3 = 8$ 个 3 元组是按相邻两个 3 元组的距离等于 1 来排列的。这也是一般 n 维立方体上 n 元组的排列规则。很显然，既然小圆点标记的 n 元组是使得布尔函数输出为 1 的 n 个输入值，所以，一个这样的 n 元组恰好对应布尔表达式的一个小项。

例如，一个 3 元布尔函数 $f(x_1, x_2, x_3) = \bar{x}_1 \oplus x_2 x_3$，它的 3 元立方体表示为图 7.7。

n 维立方体表示法的明显不便之处是当 $n > 4$ 时，n 维立方体的拓扑结构决定了直观表示是困难的。这样就有一种所谓 n 维立方体的简化表示法。我们仍遵循相邻两个顶点对应的 n 元组的海明距离为 1，并且只将对应输出为 1 的那些顶点画成一个平面图形（如图 7.8）。其实这不过是沿立方体的若干适当的棱剪开它后，再展开在一个平面上的结果。

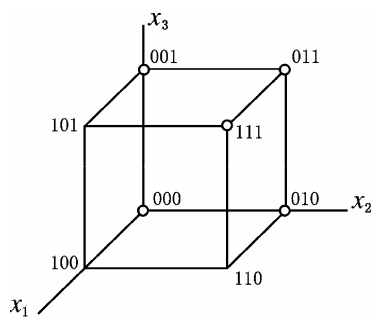


图 7.7　布尔函数的 n 维空间表示法

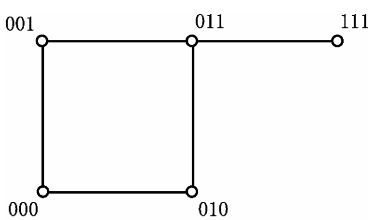


图 7.8　n 维立方体的简化表示

第四种布尔函数的表示法实际就是放弃图形的直观，用上面第三种简化 n 维立方体的所有顶点对应的 n 元输入组成的向量来表示一个布尔函数。例如，对上述函数 $f(x_1,x_2,x_3)=\bar{x}_1 \oplus x_2x_3$，可表示成(000,001,010,011,111)。这种表示法也叫做**立方体向量表示法**。向量的每一个分量是一个 n 元组，也叫做**立方体**。立方体向量表示法的一个好处是它可以编制计算机的算法以实现布尔函数的简化。

最后一种常用的布尔函数表示法是**卡诺图**，它常见于各种数字电路教科书中。不过布尔函数的卡诺图只适于用手工化简函数。

一个 n 元布尔函数的卡诺图是一个含有 2^n 个小方块的矩形。它的每一列或每一行各对应一个布尔函数的变元的输入值 0 或 1，即一个变元对应两行或两列。当 $n>2$，为使绘出的卡诺图能用二维几何图形（平面或曲面）表示，有些行或列必须重合。如图 7.9 所示。图 7.9（c）是 3 元卡诺图，它有 4 个列，是由表示 $x_1=0$ 和 $x_1=1$ 的两列与 $x_2=0$ 和 $x_2=1$ 的两列两两交错重合后产生的。我们在每一列上标出了对应变元 x_1 和 x_2 输入值的一个 0 和 1 组成的长度是 2 的串。如第 1 列被标为“00”，表示该列对应 x_1 和 x_2 的输入均为 0 的情况，第 2 列被标为“01”，表示该列对应 $x_1=0$ 和 $x_2=1$ 的情况……至于第 3 个变元 x_3 的输入，图中用两行分别表示对应它的输入值为 0 和 1 的情况。于是，卡诺图的每一个小矩形都是由若干行与若干列相交产生的。例如，第 1 行第 3 列（图中用斜线填充的小方块）是由 $x_1=1$ 和 $x_2=1$ 对应的两列与 $x_3=0$ 对应的行相交产生的小矩形，它将表示布尔函数相应输入“110”时的输出。应该说明的是，在布置这些列和行时，交错安排某两个变元对应的列或行（即以上指出的某两列或行重合的情形）是为了使得任何相邻的两小块的 n 元组（就是上述的“串”）之间的海明距离都是 1。这一点，对下一小节要介绍的极小化是至为重要的。最后，为清楚起见，在发生列或行重合的情况下，我们在表示某个变元输入为 1 的列的上（下）方特别标出该变元符号。发生行重合的情况时，可类似处理。

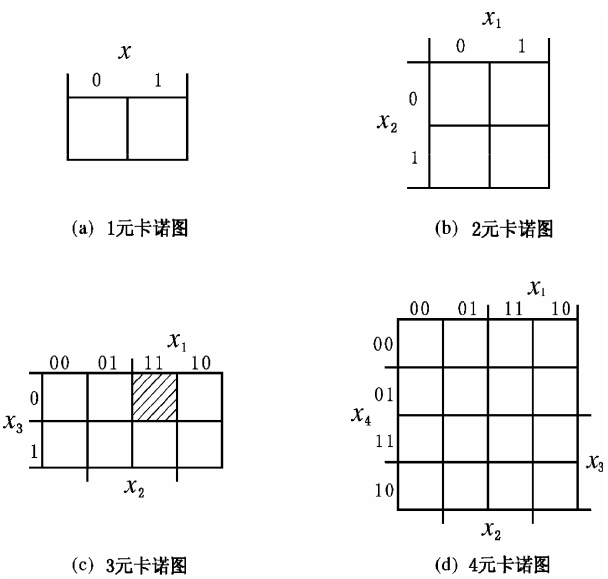


图 7.9　n 元布尔函数的卡诺图

图 7.9（d）是一个 4 元卡诺图，行的安排是和列是一样的。更进一步，若我们沿某一水平轴线将这个 4 元卡诺图“卷”成一个圆柱面，即让每一列的最上一行小块与它的最下一行

小块沿外缘对接，再将卷成的圆柱表面“不扭曲”地把它的“左”、“右”两个“圆周端口”对接在一起，这样 4 元卡诺图形成了一个“内胎”形曲面，并且分布在这个曲面上的任两个相邻小块的海明距离仍然是 1。至于 5 元卡诺图，可看成是由 2 个 4 元卡诺图“相叠”在一起构成的。图 7.10 中左边一个 4 元卡诺图上每小块与右边卡诺图对应位置上的小块的两个 5 元组分别为 $0x_2x_3x_4x_5$ 和 $1x_2x_3x_4x_5$，也就是说，它们的后 4 个输入值对应相等，只有第一个输入不同。这样，我们不仅保证位于同一 4 元卡诺图上的相邻两个小块的海明距离为 1，也保持了重叠后“上”、“下”两相邻小块的海明距离为 1。类似于上面对 4 元卡诺图所做的那样，把 5 元图的每一个 4 元卡诺图“做成”一个“内胎”，并使一个“套”在另一个外面。发挥一下想像力，读者一定会同意以下的说法：在这两个套装的“内胎”上的任意相邻两小块的海明距离都是 1。

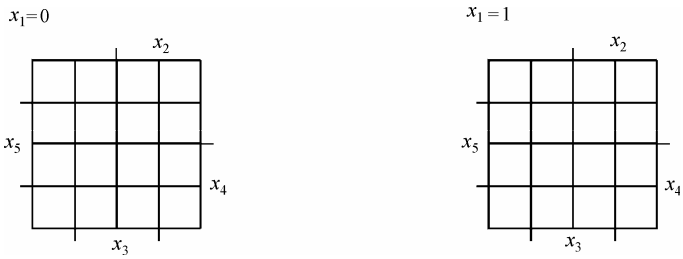


图 7.10　5 元卡诺图

至此，我们描述了所有常用的表示布尔函数的方法。

7.5.2　布尔函数的极小化

逻辑电路的设计问题一般可归纳为两个方面的工作。其一，是简化一个已存在的逻辑电路。这首先得给出该电路准确的布尔函数。其二，是由用户口头描述一个逻辑电路的功能，然后把它归纳成一个布尔函数，最后化简这个函数。在以上两种工作中，最后将简化的布尔函数中的运算“$\oplus$”、“$\cdot$”和“$\bar{\ }$”分别以相应的或门、与门和反相器（也可称做非门）等器件替代，给出简化的逻辑电路。本课程更关心的是如何简化一个布尔函数。

先来通过一个例子，看如何给出一个已存在的逻辑电路的布尔函数。

【例 7.17】　图 7.11（a）给出一个有 4 个输入端的逻辑电路。试给出它的布尔函数，并化简此电路。

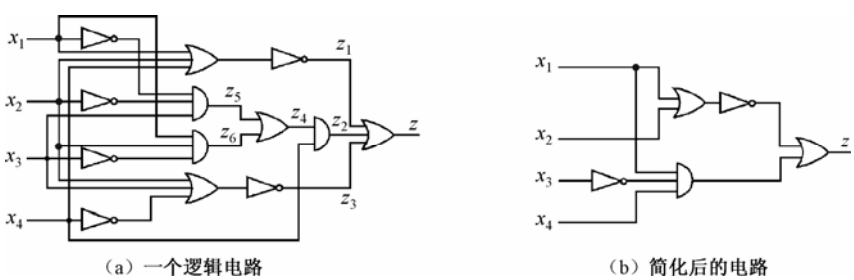


图 7.11　化简逻辑电路

解　由电路的输出端逐次向输入端反推出布尔函数。图 7.11（a）的输出是 $z = z_1 \oplus z_2 \oplus z_3$，于是

$$z_1 = \overline{(x_1 \oplus x_2 \oplus x_4)} = \bar{x}_1\bar{x}_2\bar{x}_4$$

$$z_3 = \overline{(x_2 \oplus x_3 \oplus \bar{x}_4)} = \bar{x}_2\bar{x}_3x_4$$

$$z_2 = z_4x_4 \qquad z_4 = z_5 \oplus z_6$$

$$z_5 = \bar{x}_1\bar{x}_2x_3 \qquad z_6 = x_1x_2\bar{x}_3$$

$$\begin{aligned} z &= \bar{x}_1\bar{x}_2\bar{x}_4 \oplus x_4(\bar{x}_1\bar{x}_2x_3 \oplus x_1x_2\bar{x}_3) \oplus \bar{x}_2\bar{x}_3x_4 \\ &= \bar{x}_1\bar{x}_2\bar{x}_4 \oplus \bar{x}_1\bar{x}_2x_3x_4 \oplus x_1x_2\bar{x}_3x_4 \oplus (\bar{x}_2\bar{x}_3x_4)(\bar{x}_1 \oplus x_1) \\ &= \bar{x}_1\bar{x}_2\bar{x}_4 \oplus \bar{x}_1\bar{x}_2x_3x_4 \oplus (x_1x_2\bar{x}_3x_4 \oplus x_1\bar{x}_2\bar{x}_3x_4) \oplus \bar{x}_1\bar{x}_2\bar{x}_3x_4 \\ &= \bar{x}_1\bar{x}_2\bar{x}_4 \oplus (\bar{x}_1\bar{x}_2x_3x_4 \oplus \bar{x}_1\bar{x}_2\bar{x}_3x_4) \oplus x_1\bar{x}_3x_4 \\ &= (\bar{x}_1\bar{x}_2\bar{x}_4 \oplus \bar{x}_1\bar{x}_2x_4) \oplus x_1\bar{x}_3x_4 \\ &= \bar{x}_1\bar{x}_2 \oplus x_1\bar{x}_3x_4 \\ &= \overline{(x_1 \oplus x_2)} \oplus x_1\bar{x}_3x_4 \end{aligned}$$

以上的化简中，利用了公式 $abcd \oplus abc\bar{d} = abc(d \oplus \bar{d}) = abc$ 。

最后的布尔函数对应的电路可简化为图 7.11（ b ）。

从以上的例子可见，通过布尔代数的恒等式来化简一个布尔函数需要较高的技巧。下面就介绍两种很直观的简化方法，一种以 n 维空间表示法为基础，另一种是以卡诺图为基础。而且这两种简化方法在理论上主要都基于两个布尔代数的恒等式。它们是：

$$ab \oplus \quad a\bar{b} = a \text{ 和 } ab \oplus a = a \quad ^* \qquad (7.29)$$

这就意味着在 n 维空间立方体中（参考图 7.12（a）），可以将相邻“小圆点”的对{101，001}（对应于一对小项 $\{x_1\bar{x}_2x_3, \bar{x}_1\bar{x}_2x_3\}$ ）简化成减少一个变元的初等积 { $x01$ }（消去的变元以 x 表示），即将 $\{x_1\bar{x}_2x_3, \bar{x}_1\bar{x}_2x_3\}$ 简化为 $\bar{x}_2x_3$ ，这样做的合理性基于公式（7.29）第一个公式。通常我们说，用高维的“立方体”{ $x01$ } **覆盖了**两个较之低一维度的相关“立方体”{101}和{001}。一个 n 维立方体上的一个小圆点对应一个 0 和 1 组成的 n 元组，它是一组输入值，并且在此输入下，布尔函数的输出是 1。已经说过，一个这样的小圆点，对应一个布尔函数的小项。我们把小项叫做 **0 立方体**（寓意它是一个“点”）。如{1001}，{1011}，{1101}，{1111}都是 4 元布尔函数中的 0 立方体。它们先后依次两两可复合成为 {10 x 1} 和 {11 x 1}。最后这两个可以叫做是“直线”。像这种在 0 立方体中消去了一个变元后所得的“直线”叫做 **1 立方体**。类似地，两个相关的 1 立方体可以复合成一个 2 立方体……如上述两个 1 立方体，进一步可复合成 2 立方体 {1 xx 1}。一般来说，消去了 r 个变元后的小项（或 0 立方体）是 r **立方体**，并且 r 立方体覆盖生成它的各个阶段用到的立方体。因为，如果由 { $a\bar{b}c$ } 和 { abc } 复合成 { ac }，那么由吸收律有 $ac \oplus abc = ac$ 和 $ac \oplus a\bar{b}c = ac$ 。这意味着可以用一个高阶的立方体等价地替代所有那些被它直接或间接覆盖的低阶立方体。因为，这个高阶立方体正是由这些低阶立方体逐次复合生成的。

现在再回到图 7.12（ b ），首先用两个 1 立方体（直线）{0 x 1}，{1 x 1} 各覆盖两个 0 立方体，接着再用 2 立方体（平面）{ xx1 } 去覆盖上一步生成的两个 1 立方体。这样做了以后，我们实际上已经将布尔函数 $z = \bar{x}_1\bar{x}_2x_3 \oplus \bar{x}_1x_2x_3 \oplus x_1\bar{x}_2x_3 \oplus x_1x_2x_3$ 等价地简化成了 $z = x_3$ 。

---

* 一般地，其中 a,b 都可以是一个布尔表达式。

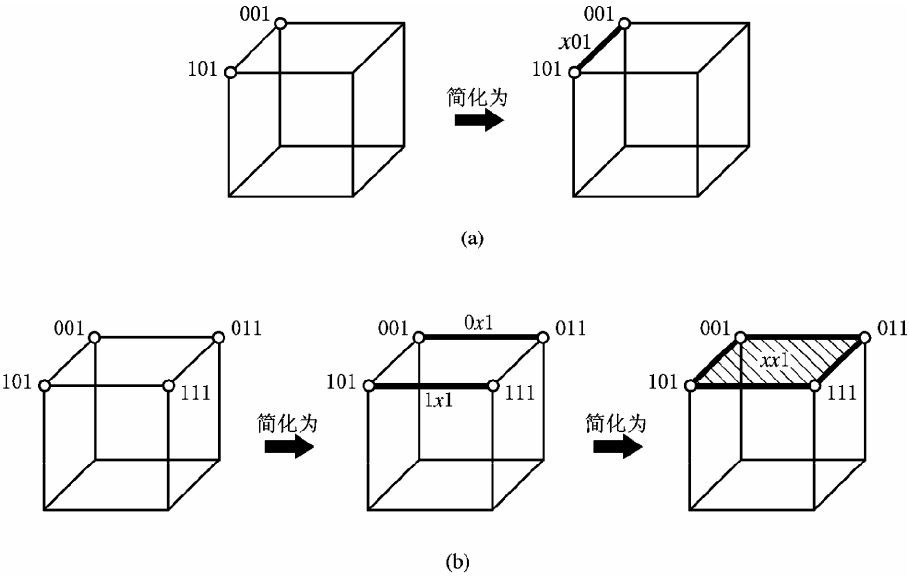


图 7.12　n 维立方体化简的几何解释

现在把基于 n 维立方体化简布尔函数的图解法归纳如下：

（1）用以下任一方法求出对应布尔函数值为 1 的所有 n 元输入组。这可以是列表法，也可以是化成主积和范式法。

（2）依据第（1）步的结果，画 n 维立方体图。

（3）在立方体图中，将相邻的顶点复合成直线；将相邻的“平行”直线（Hamming 距离为 1）复合成平面；相邻的平面复合成 3 立方体……直至没有相邻的同阶立方体为止。

（4）优先选择高阶立方体，组成一个覆盖所有 0 立方体的尽可能小的立方体集。

（5）将第（4）步生成的最小集的每一个立方体表示为初等积，以这些初等积之和求得最后化简的布尔函数。

基于卡诺图的简化方法的几何解释可以类似地来讨论。

以 5 元布尔函数 $z=\bar{x}_3(\bar{x}_5 \oplus x_1x_2x_3) \oplus x_3(\bar{x}_1x_5 \oplus x_5(x_1x_4 \oplus x_2\bar{x}_4))$ 为例。或者用列表格法，或者用求主积和范式的方法求出此布尔函数的所有小项（0 立方体）是：{00000}，{01000}，{00010}，{01010}，{00101}，{01101} 等等共 15 个。在它的卡诺图（图 7.13）上，每一 0 立方体用符号“1”标出。类似于 n 维立方体图的简化过程，可以将相邻的两个小块合并成一个 2—小项块，对应于 1 立方体（记住上一小节所说的 5 元卡诺图是一个嵌套内胎形，相邻的概念是在此意义下来理解的。本质上说，两相邻立方体的海明距离是 1）；将相邻的 2—小项块，合并成一个 4—小项块（2 立方体）……合并后的较大块若在 5 元卡诺图的同一 4 元卡诺图中（一个 5 元卡诺图由两个 4 元卡诺图组成），用实线将它围起；若属于不同 4 元卡诺图，则用虚线将它们围起。最后，此布尔函数的卡诺图合并成一个 3 立方体（跨越两个 4 元卡诺图，包容 8 个小方块），对应于初等积 $\bar{x}_3\bar{x}_5$，一个 2 立方体（在对应 $\bar{x}_1$ 的 4 元卡诺图上，包容 4 个小方块），对应于初等积 $\bar{x}_1x_3x_5$，两个 1 立方体（一个在对应 x_1 的卡诺图上，另一个跨于两个 4 元卡诺图上，它们各包容 2 个小方块），对应于下面的公式最后两项。这 4 个立方体覆盖了布尔函数所有 15 个小项。因此，化简后的布尔函数是

$$z=\bar{x}_3\bar{x}_5 \oplus \bar{x}_1x_3x_5 \oplus x_2x_3\bar{x}_4x_5 \oplus x_1x_3x_4x_5$$

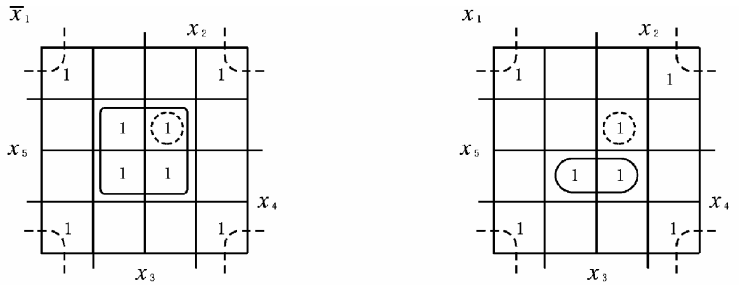


图 7.13　5 元卡诺图的简化

以上讨论了两种通过图示法化简布尔函数的方法。一般只适用于手工处理。不过，基于 n 维立方体图示法而衍生出的立方体向量表示法却适合于计算机编程处理。为此，我们要将原先由人工判断的两种操作——两同阶立方体是否相邻（海明距离是否等于 1）和从两个相邻立方体合并成高一阶的一个立方体——都用计算机来运算。为实现这两种运算，需要定义一种适合此类运算的立方体位串的新表示方法。这就是对立方体位串中的 0 用 2 位位串“01”表示；位串中的 1 用“10”来表示；而一个已被消去的变元 x，用“11”表示。例如，对 1 立方体{10 x 1}，现在被表示为｛10 01 11 10｝。这样一来，以上两种判断就可以由机器运算来实现。譬如，就立方体｛1010｝和｛1011｝，｛1 x 10｝和｛11 x 0｝，在用以上新的约定表示后，做“按位异或”的运算是

$$10\ 01\ 10\ 01 \overline{\vee} 10\ 01\ 10\ 10 = 00\ 00\ 00\ 11$$

$$10\ 11\ 10\ 01 \overline{\vee} 10\ 10\ 11\ 01 = 00\ 01\ 01\ 00$$

很显然，当异或的结果中出现连续的两个 1，其他位均为 0，并且第一个 1 出现在从位串左边第一位起计算是奇数位上时，说明原来两个立方体是相邻的，否则就是不相邻的。相邻的判断也可这样被定量地描述，即两位串按位异或的结果等于 $2^i + 2^{i+1}$（$i = 0,2,4,\cdots,2n-2$, n 是立方体的总变元数）。

再来看将两相邻立方体｛1010｝和｛1011｝按新约定表示后的“按位或”的结果

$$10\ 01\ 10\ 01 \vee 10\ 01\ 10\ 10 = 10\ 01\ 10\ 11$$

将以上结果翻译成老的立方体表示法就是｛101 x ｝，而这正是以上两个 0 立方体合并后所得的 1 立方体。

最后，我们还有一个算法，来实现搜索覆盖所有小项（或 0 立方体）的高阶立方体的最小集合。这个搜索算法被称为奎恩－麦克克拉斯克（Quine－McCluskey）算法 *。该算法可在有关文献中找到，在此不再赘述。

至此，我们已给出了利用立方体向量化简布尔函数的计算机算法的全部线索。

习　　题

7.1　由图 7.14 给出的各偏序集中，哪些是偏序格？为什么？

7.2　设 R_s 是闭区间［0，1］上的实数的集合，且≤是 R_s 上通常的“小于或等于”关系。证明：$<R_s, \leqslant>$是格。问这个格上的“和”与“积”运算各是什么？

* 参阅书末参考文献之 1。

7.3　由以下集合 L 分别构成偏序集$<L,\leqslant>$，其中$\leqslant$定义为：对于 $n_1,n_2\in L,n_1\leqslant n_2$，当且仅当 n_1 是 n_2 的因数。问其中哪些偏序集是格？

（a）$L=\{1,2,3,4,6,12\}$

（b）$L=\{1,2,3,4,6,8,12,14\}$

（c）$L=\{1,2,3,4,5,6,7,8,9,10,11,12\}$

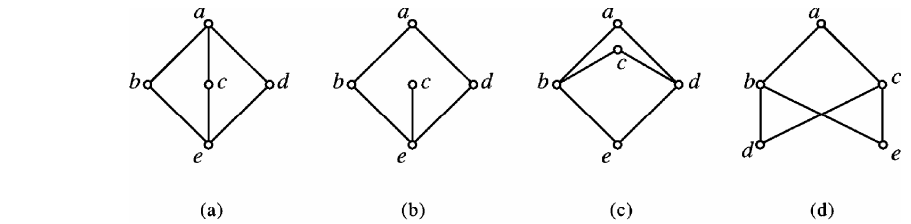


图 7.14　习题 7.1

7.4　设$<A,\leqslant>$是格，试证明$<A,\geqslant>$也是格。

7.5　说明本章式（7.13）是自对偶的。

7.6　设$<A,\leqslant>$是格，$a,b\in A$，证明：$ab<a$ 和 $ab<b$，当且仅当 a 和 b 是不可比的。（$x<y$ 就是 $x\leqslant y$ 且 $x\neq y$）。

7.7　设$<A,\leqslant>$是一个分配格，证明：如果对于 $x,y\in A$，有一个 $a\in A$ 使

$$ax=ay \quad 和 \quad a\oplus x=a\oplus y$$

则 $x=y$

7.8　设 $A=\{a,b,c\}$，试给出格$<\rho(A),\subseteq>$的 Hasse 图，并指出它的最大元和最小元、每一元素的补元以及所有原子。

7.9　设$<A,\oplus,\bullet>$是一个分配格，$a,b,c\in A$，证明：

$$(a\oplus b)c\leqslant a\oplus bc$$

（可进一步证明上式是$<A,\oplus,\bullet>$为分配格的充分条件）

7.10　证明：在格中，下面的式子成立

$$ab\oplus cd\leqslant(a\oplus c)(b\oplus d)$$

7.11　本章定理 7.10 的假设前提 $xy=xz$ 和 $x\oplus y=x\oplus z$ 是互为偶式的，于是有人说可以只用一个等式作为该定理的假设前提。你认为这样说是正确的吗？为什么？

7.12　证明本章式（7.20）和式（7.21）是等价的。因此，我们说一个格是分配格的定义可以将假设条件减弱成只有本章式（7.20）或式（7.21）之一成立。这样做是否对？为什么？试与上题做一比较。

7.13　证明：在有界格中，0 和 1 互为唯一的补元。

7.14　证明：若一个有界格含有不止一个元素，则该有界格中任一元素的补元必不是它自身。

7.15　证明：若一个全序格含有不止两个元素，则这个格必不是有补格。

7.16　设$<A$，$\leqslant>$是有界格，0 和 1 分别是其最小元和最大元。证明：对于 $x,y\in A$，

（a）若 $x\oplus y=0$，则 $x=y=0$；

（b）若 $xy=1$，则 $x=y=1$。

7.17　图 7.15 给出了一个有界格。

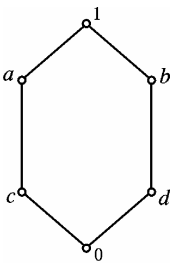


图 7.15　习题 7.17

（a）它是否有补格？为什么？

（b）现在不用逐一验证的方法，如何判断这里所有给的格是否一个分配格？

7.18　证明在布尔代数中

$$x \leqslant y \Leftrightarrow x\bar{y} = 0 \Leftrightarrow \bar{y} \leqslant \bar{x} \Leftrightarrow \bar{x} \oplus y = 1$$

7.19　证明在布尔代数中

（a）$x \oplus \bar{x}y = x \oplus y$；

（b）$x(\bar{x} \oplus y) = xy$。

7.20　设$< B, \oplus, \cdot, \bar{} >$是一个布尔代数，试证明：$< B, * >$是一可交换群，其中二元运算*的定义由下式给出：

$$x * y = \bar{x}y \oplus x\bar{y}$$

7.21　证明下列等式在布尔代数下成立。

（a）$xy \oplus x\bar{y} = x$

（b）$(x \oplus y \oplus z \oplus u)(y \oplus u) = y \oplus u$

7.22　在任意布尔代数下，证明：

（a）$x = y \Leftrightarrow \bar{x}y \oplus x\bar{y} = 0$

（b）$x = 0 \Leftrightarrow \bar{x}y \oplus x\bar{y} = y$

（c）$x \leqslant y \Rightarrow x \oplus yz = y(x \oplus z)$

（d）$(x \oplus \bar{y})(y \oplus \bar{z})(z \oplus \bar{x}) = (\bar{x} \oplus y)(\bar{y} \oplus z)(\bar{z} \oplus x)$

7.23　将以下布尔表达式化成三元主积和范式。

（a）$\overline{x_1}$

（b）$\overline{(x_1 \oplus \bar{x}_2)}(\bar{x}_2 \oplus x_3)$

7.24　化简以下布尔表达式。

（a）$\overline{xy} \oplus \overline{(x \oplus y)}$

（b）$\bar{x}\,\bar{y}z \oplus x\bar{y}z \oplus x\bar{y}\,\bar{z}$

（c）$1\,x \oplus 0\bar{x}$

（d）$(x \oplus y)x \oplus (y \oplus \bar{y})x$

7.25　将以下布尔表达式化成三元主和积表达式。

（a）x_1

（b）$x_1x_2 \oplus x_2x_3 \oplus x_3x_1$

7.26　证明：任一个布尔代数的元素个数必为 2 的正整数次幂。

7.27　设$S = \{a, b, c\}$，$< \rho(S), \cup, \cap, \sim, \phi, S >$是布尔代数。又设$g : \rho(S) \to B$，其中 B 是本章 7.3 节例 7.8 的两元素布尔代数，对$x \in \rho(S)$使得

$$g(x) = \begin{cases} 1 & \text{当} b \in x \\ 0 & \text{否则} \end{cases}$$

证明 g 是一个布尔同态。

7.28　证明：由一个布尔代数到另一个布尔代数的映射如果保持运算“$\oplus$”和“$\bar{\ }$”，则也保持乘运算“$\cdot$”。

7.29　证明：本章关于布尔同态的定义 7.14 可以将条件减弱至只要求映射保持加运算和补运算（参考本章练习题 7.28）。

7.30　试分别用卡诺图和 n 维立方体图化简布尔函数 $f(x_1,x_2,x_3,x_4,x_5)=\bar{x}_3(\bar{x}_5\oplus x_1x_2x_3)\oplus x_2(x_1\bar{x}_3x_4\oplus\bar{x}_4(x_1\oplus x_3x_5))$。

参 考 文 献

[1] （美）特伦布莱著．马诺哈，罗远诠等译．离散数学结构及其在计算机科学中的应用．上海：上海科学技术出版社，1982

[2] 马叔良等．离散数学．北京：电子工业出版社，1997

[3] 马叔良等．离散数学——学习指导及解题分析．北京：电子工业出版社，1998

[4] 徐洁盘．离散数学导论．北京：人民教育出版社，1982

[5] 左孝凌等．离散数学．上海：上海科学技术文献出版社，1987

[6] 王宪钧．数理逻辑引论．北京：北京大学出版社，1982

《离散数学（第 3 版）》读者意见反馈表

尊敬的读者：

感谢您购买本书。为了能为您提供更优秀的教材，望您将意见及时告知我们，以改进我们的服务。对采用您的意见进行修订的教材，我们将在该书的前言中进行说明并赠送您样书。

姓名：_____ 电话：_____

职业：_____ E-mail:_____

邮编：_____ 通信地址：_____

1．您对本书的总体看法是：

□很满意 □比较满意 □尚可 □不太满意 □不满意

2．您对本书的结构（章节）：□满意 □不满意 改进意见_____

3. 您对本书的例题 □满意 □不满意 改进意见_____

4．您对本书的习题 □满意 □不满意 改进意见_____

5．您对本书的实训 □满意 □不满意 改进意见_____

6． 您对本书其他的改进意见：

7．您感兴趣或希望增加的章节是：

请寄：100036 北京万寿路 173 信箱高等职业教育分社 吕迈收

电话：010-88254572 E-mail:lumai@phei.com.cn（可通过邮件索取本表电子版）